(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－177525

(43)公開日　平成10年(1998)６月30日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ｄ
Ｇ０８Ｂ　25/10		Ｇ０８Ｂ　25/10	Ｚ
Ｈ０４Ｑ　7/38		Ｈ０４Ｂ　7/26	１０９Ｒ

審査請求　未請求　請求項の数19　ＯＬ　（全 26 頁）

(21)出願番号　特願平8－335336

(22)出願日　平成８年(1996)12月16日

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地

(72)発明者　三浦　興己
神奈川県横浜市港北区網島東四丁目３番１号　松下通信工業株式会社内

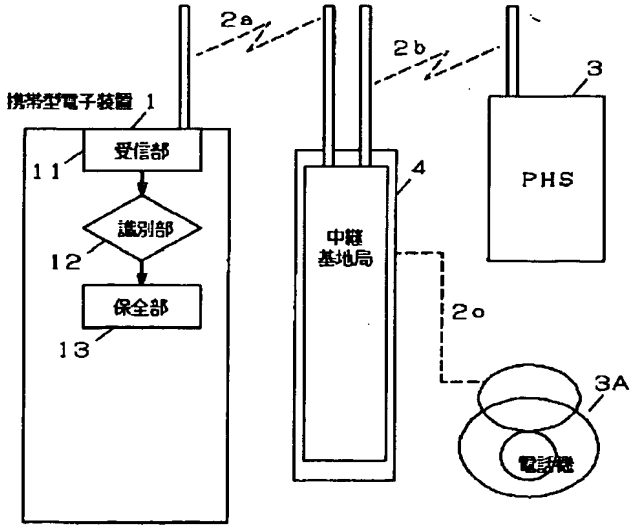
(74)代理人　弁理士　滝本　智之　（外１名）

(54)【発明の名称】　携帯型電子装置の保全システム

(57)【要約】

【課題】　盗難や紛失した携帯型電子装置の所有者や送信相手者が害を被ることを排除する。

【解決手段】　携帯型電子装置１に電波通信手段を介して送信されてくる遠隔操作データを受信する受信部１１と、受信部１１で受信した遠隔操作データを識別する識別部１２と、識別部１２による識別結果に基づいて携帯型電子装置１の所有者が害を被ることを排除する所定の保全部１３を設け、携帯型電子装置１が盗まれたり紛失した場合に、ネットワークやオンラインシステムの回線事業会社に連絡して回線の解約解除の手続きをする前に、保全部１３で保全処理することにより、携帯型電子装置の所有者の財産または情報に関わるセキュリティを高めることを可能にする。



1

【特許請求の範囲】

【請求項１】　携帯型電子装置に電波通信手段を介して送信されてくる遠隔操作データを受信する受信手段と、前記受信手段で受信した遠隔操作データを識別する識別手段と、前記識別手段による識別結果に基づいて携帯型電子装置の所有者が害を被ることを排除する所定の保全処理手段を設け、携帯型電子装置の所有者の財産または情報に関わるセキュリティを高めることを特徴とする携帯型電子装置の保全システム。

【請求項２】　携帯型電子装置が盗まれたり紛失した時に電波通信手段を介して送信されてきた遠隔操作データの識別結果により、携帯型電子装置の所有者が害を被ることを排除する所定のセキュリティを高める保全処理手段を設けたことを特徴とする請求項１記載の携帯型電子装置の保全システム。

【請求項３】　電波通信手段を介して送信されてくる遠隔操作データ受信し、該遠隔操作データの識別結果により、携帯型電子装置の所有者に送信した相手または相手情報が害を被ることを排除する保全処理手段を１つまたは１つ以上設けたことを特徴とする請求項２記載の携帯型電子装置の保全システム。

【請求項４】　保全処理手段は、携帯型電子装置の所有者が予め入力したキーワードを記憶する第１記憶手段と、電波通信手段を介して送信される遠隔操作データを受信し、該遠隔操作データの識別結果のキーワード情報を記録する第２記録手段、前記第１記憶手段のキーワードと前記第２記録手段のキーワード情報との一致を確認した後、保全処理を実行することを特徴とする請求項２または３記載の携帯型電子装置の保全システム。

【請求項５】　保全処理手段の保全処理内容として、盗難や紛失された携帯型電子装置を所有者以外の他人が使用しようとしても、携帯型電子装置の本来の機能を停止して他人が使用できなくする「電源オフ」の保全処理を行うことを特徴とする請求項３記載の携帯型電子装置の保全システム。

【請求項６】　保全処理手段の保全処理内容として、盗難や紛失された携帯型電子装置を所有者以外の他人が使用すると、視覚または聴覚によりアラームを発生して使用を禁止する「警告発生」の保全処理を行うことを特徴とする請求項３記載の携帯型電子装置の保全システム。

【請求項７】　保全処理手段の保全処理内容として、盗難や紛失された携帯型電子装置を所有者以外の他人が使用すると、所有者が予め入力して記憶手段に記憶した連絡先やメッセージを表示し、携帯型電子装置を回収する「メッセージ表示」の保全処理を行うことを特徴とする請求項３記載の携帯型電子装置の保全システム。

【請求項８】　保全処理手段の保全処理内容として、盗難や紛失された携帯型電子装置を所有者以外の他人が使用すると、本来の機能を停止し、所有者が予め入力して記憶手段に記憶した連絡先にのみ交信する「所有者連絡

2

発信」の保全処理を行うことを特徴とする請求項３記載の携帯型電子装置の保全システム。

【請求項９】　保全処理手段の保全処理内容として、盗難や紛失された携帯型電子装置の本来の機能のうち所有者が予め入力した機能を停止する「発信機能禁止」の保全処理を行うことを特徴とする請求項３記載の携帯型電子装置の保全システム。

【請求項１０】　保全処理手段の保全処理内容として、盗難や紛失された携帯型電子装置の記録手段からデータの出力を禁止する「データ出力禁止」の保全処理を行うことを特徴とする請求項３記載の携帯型電子装置の保全システム。

【請求項１１】　保全処理手段の保全処理内容として、盗難や紛失された携帯型電子装置の記録手段のデータを消去し、他人に見られたり使用されないようにする「記憶データ消去」の保全処理を行うことを特徴とする請求項３記載の携帯型電子装置の保全システム。

【請求項１２】　保全処理手段の保全処理内容として、盗難や紛失された携帯型電子装置の通信回線番号を消滅し、他人が使用できなくする「通信回線番号消滅」の保全処理を行うことを特徴とする請求項３記載の携帯型電子装置の保全システム。

【請求項１３】　保全処理手段の保全処理内容として、盗難や紛失された携帯型電子装置の記録手段のデータを他の所定の電子装置に転送し、記憶データを回収する「記憶データ転送」の保全処理を行うことを特徴とする請求項３記載の携帯型電子装置の保全システム。

【請求項１４】　保全処理手段の保全処理内容として、使用者の識別手段により使用者を識別し、所有者以外の他人が携帯型電子装置の使用を不可能にする「保全処理」を行うことを特徴とする請求項３記載の携帯型電子装置の保全システム。

【請求項１５】　送信した相手または相手情報に対する保全処理手段は、遠隔操作データによって、

ａ．携帯型電子装置に送信した相手に、所有者が受信できない事情にある所定の情報を相手に送信する保全処理と、

ｂ．携帯型電子装置に送信した相手からの受信情報を受信する機能を停止する保全処理と、

ｃ．携帯型電子装置に送信した相手に、話中または使用中のデータを送信する保全処理と、

ｄ．携帯型電子装置に送信した相手に、送信情報を送信する機能を停止する保全処理と、

ｅ．携帯型電子装置に送信した相手に、所有者が予め入力して記憶手段に蓄積記憶した紛失メッセージを送信する保全処理と、

ｆ．携帯型電子装置に送信した相手に、該携帯型電子装置の保全システムの使用を防止する保全処理と、のうち１つ以上の処理を実施することを特徴とする請求項３記載の携帯型電子装置の保全システム。

【請求項１６】　電波通信手段を伝送媒体にして、所有者が予め入力して記憶手段に記憶したキーワード信号を受信した場合に、遠隔操作データの識別結果により、強制的に携帯型電子装置の保全処理手段を駆動し、所有者が害を被ることを排除する所定のセキュリティを高める保全処理を行うことを特徴とする請求項５乃至１４の何れかに記載の携帯型電子装置の保全システム。

【請求項１７】　所有者が予め入力して記憶手段に記憶した呼び出し信号回数のパターンを受信した場合に、遠隔操作データの識別結果により、強制的に携帯型電子装置を接続し、所有者が害を被ることを排除する所定のセキュリティを高める保全処理を行うことを特徴とする請求項５乃至１４の何れか１項に記載の携帯型電子装置の保全システム。

【請求項１８】　携帯型電子装置に保全処理を促すための発振手段、該発振手段の発振信号を送信する微弱電力送信手段を有する携帯型電子装置の子機と、該子機からの保全処理を促すための発振データを受信する微弱電力受信手段、該微弱電力受信手段で受信した操作データを識別する識別手段、該識別手段の識別結果により携帯型電子装置の所有者が害を被ることを排除する所定の保全手段を揺する本体を備え、携帯型電子装置の所有者の財産または情報に関わるセキュリティを高めることを特徴とする携帯型電子装置の保全システム。

【請求項１９】　携帯型電子装置との間で交信する微弱電力伝送手段、該微弱電力伝送手段の受信信号から携帯型電子装置との間の距離を判別する判別手段、該判別手段による所定の距離より離れた判別結果により保全処理を促すための発振データを前記微弱電力伝送手段で受信し、該発振データにより警告音を発生する手段を有する携帯型電子装置の子機と、前記子機と同様の双方の微弱電力伝送手段、子機との間の距離を判別する判別手段、該判別手段による所定の距離より離れた判別結果により保全処理を起動し、警告音を発生する手段を有する本体を備え、紛失あるいは盗難および置き忘れを防止することを特徴とする携帯型電子装置の保全システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、携帯型電子装置（ＰＨＳ、携帯電話機も含む電波通信手段を有するデータ処理端末装置をいう）の盗難や紛失に対して所有者が害を被ることを排除し、所定のセキュリティを高める保全処理機能を備えた携帯型電子装置の保全システムに関する。

【０００２】

【従来の技術】従来、上記のような携帯型電子装置は、その装置の特色上、広い不特定領域の屋外に持ち出して使用される。また、通信回線を登録した携帯型電子装置は、ＰＨＳ（Personal Hanndy Phone System）、そのデータ処理端末装置などデジタル信号情報のコンピュータ周辺端末装置として用途が拡大するとともに、その持ち出し使用領域を広げていくことができる。また、その使用方法も容易で、多くの人々の需要がある。

【０００３】

【発明が解決しようとする課題】しかしながら、この種従来の携帯型電子装置は、所有者がその装置自体を屋外などに持ち出して使用したり、手軽に携帯できるため、盗難や紛失する機会が多く、盗難や紛失したこの種の携帯型電子装置を他人が拾得した場合にも、容易に使用できる可能性があり、元々の所有者はプライベイト情報や重要データを盗み見されたり、使用していない通話料金などの請求を請けるなど所有者が害を被る問題が発生している。

【０００４】また、盗難や紛失した携帯型電子装置の所有者に送信した相手にとっても、不適切な状況であることを知らずに携帯型電子装置の所有者と思って送信したことで、送信相手または相手情報が害を被る問題が発生するおそれもある。

【０００５】本発明は、このような従来の問題点を解決するものであり、盗難や紛失した携帯型電子装置の所有者や送信相手者が害を被ることを排除できる携帯型電子装置の保全システムを提供することを目的とするものである。

【０００６】

【課題を解決するための手段】この課題を解決するために本発明は、携帯型電子装置に電波通信手段を介して送信されてくる遠隔操作データを受信する受信手段と、前記受信手段で受信した遠隔操作データを識別する識別手段と、前記識別手段による識別結果に基づいて携帯型電子装置の所有者が害を被ることを排除する所定の保全処理手段を設けたものである。

【０００７】これにより、盗難や紛失した携帯型電子装置の所有者や送信相手者が害を被ることを排除できる。

【０００８】

【発明の実施の形態】本発明の請求項１に記載の発明は、携帯型電子装置に電波通信手段を介して送信されてくる遠隔操作データを受信する受信手段と、前記受信手段で受信した遠隔操作データを識別する識別手段と、前記識別手段による識別結果に基づいて携帯型電子装置の所有者が害を被ることを排除する所定の保全処理手段を設けることにより、盗難や紛失した携帯型電子装置の所有者や送信相手者が害を被ることを排除でき、携帯型電子装置の所有者の財産または情報に関わるセキュリティを高めることが可能になる。

【０００９】本発明の請求項２に記載の発明は、携帯型電子装置が盗まれたり紛失した時に電波通信手段を介して送信されてきた遠隔操作データの識別結果により、携帯型電子装置の所有者が害を被ることを排除する所定のセキュリティを高める保全処理手段を設けることにより、盗難や紛失した携帯型電子装置の所有者や送信相手

者が害を被ることを排除でき、携帯型電子装置の所有者の財産または情報に関わるセキュリティを高めることが可能となる。

【００１０】本発明の請求項３に記載の発明は、電波通信手段を介して送信されてくる遠隔操作データ受信し、該遠隔操作データの識別結果により、携帯型電子装置の所有者に送信した相手または相手情報が害を被ることを排除する保全処理手段を１つまたは１つ以上設けることにより、盗難や紛失した携帯型電子装置の所有者や送信相手者が害を被ることを排除でき、携帯型電子装置の所有者の財産または情報に関わるセキュリティを高めることが可能となる。

【００１１】本発明の請求項４に記載の発明は、保全処理手段が、携帯型電子装置の所有者が予め入力したキーワードを記憶する第１記憶手段と、電波通信手段を介して送信される遠隔操作データを受信し、該遠隔操作データの識別結果のキーワード情報を記録する第２記録手段、前記第１記憶手段のキーワードと前記第２記録手段のキーワード情報との一致を確認した後、保全処理を実行することにより、携帯型電子装置を使用する折に、個々のキーワードを入力しなければ動作せず、所有者の大切な登録情報を保全・安全・確実を保証するセキュリティが保たれ、個別のキーワードの適用により厳格に守る仕組みが成り立ち、盗難や紛失での管理作業での誤りを生ずることが回避でき、登録情報やその管理のセキュリティを高めることができる。

【００１２】本発明の請求項５に記載の発明は、保全処理手段の保全処理内容として、盗難や紛失された携帯型電子装置を所有者以外の他人が使用しようとしても、携帯型電子装置の本来の機能を停止して他人が使用できなくする「電源オフ」の保全処理を行うことにより、電源が入らなくなるので携帯型電子装置の基本機能を殺す保全処理がなされ、携帯型電子装置の紛失者にとって最小限の損失に抑えることができる。

【００１３】本発明の請求項６に記載の発明は、保全処理手段の保全処理内容として、盗難や紛失された携帯型電子装置を所有者以外の他人が使用すると、視覚または聴覚によりアラームを発生して使用を禁止する「警告発生」の保全処理を行うことにより、携帯型電子装置の拾得者に警告発生することで携帯型電子装置の使用を禁止する保全処理が可能になり、携帯型電子装置の紛失者にとって他人に使用することを防止できる。

【００１４】本発明の請求項７に記載の発明は、保全処理手段の保全処理内容として、盗難や紛失された携帯型電子装置を所有者以外の他人が使用すると、所有者が予め入力して記憶手段に記憶した連絡先やメッセージを表示し、携帯型電子装置を回収する「メッセージ表示」の保全処理を行うことにより、携帯型電子装置の拾得者にメッセージ表示するから、携帯型電子装置の返却を訴える保全処理が可能になり、携帯型電子装置の紛失者にとって他人に使用することを防止でき、携帯型電子装置の返却が可能になる。

【００１５】本発明の請求項８に記載の発明は、保全処理手段の保全処理内容として、盗難や紛失された携帯型電子装置を所有者以外の他人が使用すると、本来の機能を停止し、所有者が予め入力して記憶手段に記憶した連絡先にのみ交信する「所有者連絡発信」の保全処理を行うことにより、携帯型電子装置の拾得者の使用に対し所有者連絡発信で連絡が取れるから、携帯型電子装置の紛失者にとって他人に使用することを防止でき、携帯型電子装置の返却が可能になる。

【００１６】本発明の請求項９に記載の発明は、保全処理手段の保全処理内容として、盗難や紛失された携帯型電子装置の本来の機能のうち所有者が予め入力した機能を停止する「発信機能禁止」の保全処理を行うことにより、携帯型電子装置の拾得者の使用に対し発信機能禁止ができるから、携帯型電子装置の紛失者にとって他人に使用することを防止でき、不当な使用による料金が生じるのを回避できる。

【００１７】本発明の請求項１０に記載の発明は、保全処理手段の保全処理内容として、盗難や紛失された携帯型電子装置の記録手段からデータの出力を禁止する「データ出力禁止」の保全処理を行うことにより、携帯型電子装置内の個人データや情報を保護するデータ出力禁止がかかるから、携帯型電子装置の紛失者にとって他人に使用することを防止でき、不当な使用による料金が生じるのを回避できる。

【００１８】本発明の請求項１１に記載の発明は、保全処理手段の保全処理内容として、盗難や紛失された携帯型電子装置の記録手段のデータを消去し、他人に見られたり使用されないようにする「記憶データ消去」の保全処理を行うことにより、携帯型電子装置内の個人データや情報を保護する記憶データ消去ができるから、携帯型電子装置の紛失者にとって他人に使用することを防止でき、不当な使用による料金が生じるのを回避できるほか、個人データや情報を悪用されるこを阻止できる。

【００１９】本発明の請求項１２に記載の発明は、保全処理手段の保全処理内容として、盗難や紛失された携帯型電子装置の通信回線番号を消滅し、他人が使用できなくする「通信回線番号消滅」の保全処理を行うことにより、携帯型電子装置の拾得者の使用に対し通信回線番号消滅ができるから、携帯型電子装置の紛失者にとって他人に使用することを防止でき、不当な使用による料金が生じるのを回避することができる。

【００２０】本発明の請求項１３に記載の発明は、保全処理手段の保全処理内容として、盗難や紛失された携帯型電子装置の記録手段のデータを他の所定の電子装置に転送し、記憶データを回収する「記憶データ転送」の保全処理を行うことにより、携帯型電子装置内の個人データや情報を遠隔操作でデータ転送できるから、携帯型電

子装置内の個人データや情報を回収でき、携帯型電子装置内の記憶データを消去できるから、携帯型電子装置の紛失者にとって他人に使用することを防止でき、不当な使用による料金が生じるのを回避できる。

【００２１】本発明の請求項１４に記載の発明は、保全処理手段の保全処理内容として、使用者の識別手段により使用者を識別し、所有者以外の他人が携帯型電子装置の使用を不可能にする「保全処理」を行うことにより、携帯型電子装置が盗まれたり紛失しても、携帯型電子装置の個人データの保護や他人に使用されることを排除する所定のセキュリティを高め得る。

【００２２】本発明の請求項１５に記載の発明は、送信した相手または相手情報に対する保全処理手段は、遠隔操作データによって、ａ．携帯型電子装置に送信した相手に、所有者が受信できない事情にある所定の情報を相手に送信する保全処理と、ｂ．携帯型電子装置に送信した相手からの受信情報を受信する機能を停止する保全処理と、ｃ．携帯型電子装置に送信した相手に、話中または使用中のデータを送信する保全処理と、ｄ．携帯型電子装置に送信した相手に、送信情報を送信する機能を停止する保全処理と、ｅ．携帯型電子装置に送信した相手に、所有者が予め入力して記憶手段に蓄積記憶した紛失メッセージを送信する保全処理と、ｆ．携帯型電子装置に送信した相手に、該携帯型電子装置の保全システムの使用を防止する保全処理のうち１つ以上の処理を実施することにより、携帯型電子装置が盗難や紛失された場合には、携帯型電子装置の保全システムの所有者が予め入力したキーワードを蓄積記憶させておき、電波通信を媒体にし遠隔操作でそのキーワードデータを他の電送装置から送信すると、キーワード情報との一致を確認した後で、保全処理を実行することができ、所有者の大切な登録情報を保全・安全・確実を保証するセキュリティが保たれるものであり、盗難や紛失しても他人に悪用される危険を回避できる。

【００２３】本発明の請求項１６に記載の発明は、電波通信手段を伝送媒体にして、所有者が予め入力して記憶手段に記憶したキーワード信号を受信した場合に、遠隔操作データの識別結果により、強制的に携帯型電子装置の保全処理手段を駆動し、所有者が害を被ることを排除する所定のセキュリティを高める保全処理を行うことにより、携帯型電子装置の紛失者が予め入力して記憶手段に蓄積記憶したキーワード信号を送信し、強制的に携帯型電子装置の保全機能を駆動し、装置の紛失者にとって他人に使用されることを防止できる。

【００２４】本発明の請求項１７に記載の発明は、所有者が予め入力して記憶手段に記憶した呼び出し信号回数のパターンを受信した場合に、遠隔操作データの識別結果により、強制的に携帯型電子装置を接続し、所有者が害を被ることを排除する所定のセキュリティを高める保全処理を行うことにより、携帯型電子装置の拾得者が応答しなとか、交信ができない事態の場合においても、呼び出し信号回数のパターンによる遠隔保全処理を起動させ、装置の紛失者にとって他人に使用されることを防止できる。

【００２５】本発明の請求項１８に記載の発明は、携帯型電子装置に保全処理を促すための発振手段、該発振手段の発振信号を送信する微弱電力送信手段を有する携帯型電子装置の子機と、該子機からの保全処理を促すための発振データを受信する微弱電力受信手段、該微弱電力受信手段で受信した操作データを識別する識別手段、該識別手段の識別結果により携帯型電子装置の所有者が害を被ることを排除する所定の保全手段を掻する本体を備えることにより、未然に紛失または置き忘れを防止し回避することができ、また所有者が携帯型電子装置を紛失または置き忘れてしまった場合でも、自動的に本体に保全処理を促すための各種の保全機能を起動させるため、他人に拾得されても装置の所有者の財産または情報に関わるセキュリティを高めることが簡単に実施できる。

【００２６】本発明の請求項１９に記載の発明は、携帯型電子装置との間で交信する微弱電力伝送手段、該微弱電力伝送手段の受信信号から携帯型電子装置との間の距離を判別する判別手段、該判別手段による所定の距離より離れた判別結果により保全処理を促すための発振データを前記微弱電力伝送手段で受信し、該発振データにより警告音を発生する手段を有する携帯型電子装置の子機と、前記子機と同様の双方の微弱電力伝送手段、子機との間の距離を判別する判別手段、該判別手段による所定の距離より離れた判別結果により保全処理を起動し、警告音を発生する手段を有する本体を備えることにより、携帯型電子装置を紛失または置き忘れを防止するための携帯型電子装置の保全システムを容易に実施することができ、携帯型電子装置を紛失または置き忘れを防止できる。

【００２７】以下、本発明の実施の形態について、図面を参照して説明する。

（実施の形態１）図１は、本発明の請求項１に対応する実施の形態１における携帯型電子装置の保全システムの構成図である。同図において、１は例えばＰＨＳ（Personal Handy Phone System）データ通信装置や携帯電話としての携帯型電子装置、２ａ，２ｂ，２ｃは公衆回線網などに接続された通信回線などの電波通信手段、３は公衆回線網などに接続された一般公衆電話や携帯電話としてのＰＨＳなど電話機、４は中継基地局である。更に電話機３Ａは公衆回線網などに接続された中継基地局４から無線通信回線２ｂを介した別のＰＨＳデータ通信装置や携帯電話としてのＰＨＳを構成する。

【００２８】携帯型電子装置１は、電波通信手段２ａを伝送媒体にし遠隔操作データを受信する受信部１１、受信した遠隔操作データを識別する識別部１２、この識別部１２の識別結果により携帯型電子装置１の所有者が害

を被ることを排除する所定の保全部１３を備え、携帯型電子装置１の所有者の財産または情報に関わるセキュリティを行い、携帯型電子装置所有者の財産または情報を保全する。

【００２９】市内や市外の一般公衆電話３から公衆回線網２ｂを介して、またＰＨＳデータ通信装置や携帯電話としてのＰＨＳ３Ａから無線通信回線２ｃを介して保全を要する携帯型電子装置１に遠隔操作データを送信する。該携帯型電子装置１は該遠隔操作データを受信部１１で受信し、受信した遠隔操作データが予め記憶された所定の遠隔操作データと一致したかを識別部１２が判別する。識別部１２では、その識別結果により一致が確認された場合のみ保全部１３が携帯型電子装置１の所有者が害を被ることを排除するために所定の保全処理を行う。

【００３０】次に、図４は携帯型電子装置のネットワークシステムを示す構成図であり、公衆ならびに専用回線網３０には、交換機を介して一般の電話機３１が接続されているとともに、変復調器（MODEM)付きのパソコン３２、携帯型電子装置の多数の基地局３３～３５および網管理局３６が接続される。多数の基地局３３～３５には個々の携帯型電子装置が無線通信回線を介し接続される。例えば、基地局３３には無線通信回線を介して携帯型パソコン、無線通信パソコン、無線通信電子手帳が接続され、基地局３４は無線通信回線を介して携帯型電話機、ＰＨＳ、目線通信機が接続され、基地局３５は無線通信回線を介して携帯型情報端末機が接続されている。また、網管理局３６は網全体を制御し管理するもので、各端末に対しての制御を行なう。

【００３１】個々の携帯型電子装置は保全機能を備えており、この保全機能は、その所有者より送信された遠隔操作データを受信した場合、この遠隔操作データに基づいて携帯型電子装置の所有者に不利益になる要因を排除する所定の保全処理を実行するための制御や、キーワードの入力や解析処理を実施するための制御を行ない、また異なった入力に対しても設定された保全処理を実施するための制御を行う。

【００３２】したがって、本発明の実施の形態１では、携帯型電子装置は電波通信手段と伝送媒体を通して遠隔操作データを受信部１１、受信した遠隔操作データを識別する識別部１２、この識別部１２の識別結果により携帯型電子装置の所有者が害を被ることを排除する保全部１３により、携帯型電子装置の所有者の財産または情報に関わるセキュリティを高めることができるという効果がある。

【００３３】（実施の形態２）図２は、本発明の請求項２に対応する実施の形態２における携帯型電子装置の保全システムの構成を示す、例えばＰＨＳ端末の機能ブロック図であり、キー基板とＲＦ基板で構成される。同図において、モデム部２２１は、音声符号をの適応予測と適応量子化により圧縮／伸張するＡＤＰＣＭコーディック２２１１、バッファー２２１２、フレームプロセッサ２２１３、π/4ＱＰＳＫ変調器２２１４及びπ/4ＱＰＳＫ復調器２２１５を備え、ＡＤＰＣＭコーディック２２１１にはＰＣＭコーディック２２８を介してスピーカ２３３及びマイク２３４が接続されている。また、２３５はバッテリ、２３６は電圧安定器、２３７は各回路へ電源を供給する電源回路である。

【００３４】プロトコール・プロセッサ部２３０は、所定のプロトコールに従い携帯型電子装置を制御するもので、ＣＰＵとメモリ等から構成される。図３はプロトコール・プロセッサ部の構成を示している。同図において、プロトコール・プロセッサ部２３０は、ＣＰＵ（制御部）２３０１、プロトコール・プロセッサ２３０２、カレンダ時計，タッチパネル，表示部Ｉ／Ｆ，赤外線Ｉ／Ｆ，シリアルＩ／Ｆ，ＰＣカードＩ／Ｆ，音声発生Ｉ／Ｆ，各種センサＩ／Ｆ，各種入力Ｉ／Ｆ等に対するマンマシンＩ／Ｆプロセッサ２３０３、ＲＡＭ，ＲＯＭ，Ｆ－ＲＯＭの相当するメモリ２３０４、保全処理部２３０５、発信機能，送信機能，転送機能を発揮するプロトコルプロセッサ２３０６、ＲＦコントローラ２３０７及び電源制御部２３０８を備え、マンマシンＩ／Ｆプロセッサ２３０３にはキーパット２３１及びＬＣＤドライブ２３２が接続されている。

【００３５】この構成において、無線送受信部はアンテナ２０１に到来する電波を受信側に選択された送受信切替用のＦＥＴスイッチ２０２を経由し、受信帯域のバンドパスフィルタ（ＢＰＦ）２０３で選択された後、ＬＮＡ（ローノイズアンプ）２０４で増幅される。このＬＮＡ２０４にはアッテネータが内蔵され、強電界での信号入力時にはアッテネータに切り換えることによって受信回路の飽和を防ぎ広いダイナミックレンジを確保する。ＬＮＡ２０４で増幅された信号は、送受信切替用のＦＥＴスイッチ２０５を介して、もう１段のバンドパスフィルタ（ＢＰＦ）２０６に送出され、このＢＰＦ２０６でイメージなどの不要電波を除去した後、送受信切替用のＦＥＴスイッチ２０７を介して第１ミキサ２０８へ送られる。

【００３６】第１ミキサ２０８では、受信信号と、発振部（ＴＣＸＯ）の発振信号を基にシンセサイザ２１０からアンプ２１１を通して得られる第１ローカル信号とをミキシングし、周波数チャネルの選択を行なうとともに248.45ＭＨｚの中間周波数へ変換する。このミキサ２０８は相互変調による耐妨害特性を高めるため、高いインターセプトポイントを有する。ミキサ２０８の出力は、送受信切替用のＦＥＴスイッチ２１２を介して狭帯域フィルタ特性のＳＡＷフィルタ（ＢＰＦ）２１３を経由して出力される。このＳＡＷフィルタ２１３は隣接チャネルの選択度およびイメージ妨害特性を決定し、同時に優れた群遅延特性を有する。ＳＡＷフィルタの代用として

アナログコードレス用のヘリカルフィルタを使用した場合は、イメージ周波数のみ減衰させ、次段の中間周波数で除去する。

【００３７】ＳＡＷフィルタ２１３を通過した信号は送受信切替用のＦＥＴスイッチ２１４を介して第２ミキサ２１５に入力され、ローカル発振器２１８からの信号とミキシングすることにより10.75 MHz に変換させる。第２イメージ妨害はＳＡＷフィルタ２１３の能力のみで決まるため、第２ミキサ２１５はイメージリジェクトタイプのものである。これによりＳＡＷフィルタ２１３のイメージ除去能力は緩和する。10.75 MHz のＩＦ信号はバンドパスフィルタ（ＢＰＦ）２１６通過した後、第３ミキサ２１７でローカル発振器２１８からの信号とミキシングされ、さらにバンドパスフィルタ（ＢＰＦ）２１９を通過させることで1.15MHｚに変換する。そして、リミッタ２２０で検出された信号はモデム部２２１に送られる。

【００３８】一方、モデム部２２１のπ/4ＱＰＳＫ変調器２２１４で作られたπ/4ＱＰＳＫ変調波は、デジタルデータとして図示省略のＤ／Ａコンバータに入力される。Ｄ／Ａコンバータでは10.75 MHz の変調波となり、バンドパスフィルタ（ＢＰＦ）２２２で不要信号が除去される。10.75 MHz のＩＦ信号は送信用ミキサ２２３に入力され、ローカル発振器２１８からの信号とミキシングすることにより248.45MHｚに変換される。この送信側のＩＦ信号は受信と共用したＳＡＷフィルタ２１３を通すことによりイメージなどの不要信号を除去した後、送受信切替用のＦＥＴスイッチ２１２及びパワー調整部２２４を介して送信用ミキサ２２５へ入力される。このミキサ２２５はシンセサイザ２１０からの第１ローカル信号とミキシングされ、送信周波数に変換する。この信号は、受信と共用する帯域通話フィルタ２０６を通してパワーアンプ２２６に入力される。このパワーアンプ２２６では必要なパワーに信号を増幅し、増幅された信号はローパスフィルタ（ＬＰＦ）２２７で高周波分が除去され、送信切替用のＦＥＴスイッチ２０２を経由してアンテナ２０１から放射される。

【００３９】一方、マイク２３４から入力された音声信号はＰＣＭコーデッィック２２８でデジタル化され、64 Kbpsで入力されるＰＣＭ信号をＡＤＰＣＭコーディック２２１１でＡＤＰＣＭ変換（圧縮）し、32Kbpsのデータにする。このデータは一旦バッファ２２１２に一時記憶させた後、フレームプロセッサ２２１３でＴＤＭＡフレームに構成する。このときにユニークワード、ＣＩ、ＳＡ、ＣＲＣ等の付加情報が加わるため、384 Kbps までデータレートは増加する。このデータをπ/4ＱＰＳＫ変調器２２１４で10.75 MHz の変波として図示省略のＤ／Ａコンバータに入力する。一方、1.15MHｚの受信データはπ/4ＱＰＳＫ復調器２２１５で検波され、ＡＤＰＣＭコーディック２２１１で64Kbpsに伸張され、ＰＣＭコーディック２２８でＤ／Ａ変換されてスピーカ２３３へ出力される。その他に、送信／受信の切り替えタイミングの制御、ＲＳＳＩの検出判定、ＡＦＣ制御やシンセサイザデータの設定、及び無線系のコントロールを行う。また、本実施の形態２の場合、遠隔操作データを受信した時には、この受信した遠隔操作データに基づき携帯型電子装置の所有者が害を被ることを排除する保全処理部２３０５を制御し、携帯型電子装置の所有者の財産または情報に関わるセキュリティを高める保全処理を実行すべき制御を行う。

【００４０】次に、携帯型電子装置の所有者が携帯型電子装置を盗まれたり紛失した場合について述べる。この場合は、図５に示すセキュリティを高める保全処理の制御ルーチンを実行する。まず、ステップＳ１０において、携帯型電子装置の所有者は網管理局３６に対して変復調器（ＭＯＤＥＭ）を介しパソコン３２を用いて所有する携帯型電子装置に対して通信を開始すべく遠隔操作データを入力する。この場合、携帯型電子装置が携帯していない状況（盗難や紛失）および内部に記憶されている情報の重要度により送信する遠隔操作データの内容を選択する。遠隔操作データには制御コードが所有者のみが事前に付加しており、所有者のみが知っているキーワードがある。したがって、所有者以外の例えば拾得者が任意に所有者の携帯型電子装置に対して遠隔操作データを送ることや解除することはできない。これにより遠隔操作の悪用を防止できる。

【００４１】また、携帯型電子装置のネットワークシステムで、携帯型電子装置の所有者がパソコン３２を保有していないような場合、または保有していても網管理局３６に対して変復調器（ＭＯＤＥＭ）を介し駆動するシステムになっていない時は、公衆回線網３０の一般の電話機３１により携帯型電子装置の基地局３４に遠隔操作データの送信を依頼する。またはプッシュ回線により遠隔操作データを入力する。

【００４２】次のステップＳ１１では、携帯型電子装置の所有者が入力した遠隔操作データを公衆ならびに専用回線網３０を介して携帯型電子装置の基地局３４に転送する。次のステップＳ１２では、携帯型電子装置の基地局３４より無線で遠隔操作データを送信する。

【００４３】以上のようにパソコン３２より入力した遠隔操作データが公衆ならびに専用回線網３０を介して携帯型電子装置の基地局３４に送られ、目的の所有者の手元にない所有者の携帯型電子装置に送信される。なお、携帯型電子装置が双方向二重通損の機能を有しておれば、リンクが確立し所有者の操作するパソコン３２へ携帯型電子装置の受信が確実に実行されたことを伝送する。

【００４４】したがって、本実施の形態２では、電波通信手段を伝送媒体にし受信した遠隔操作データの識別結果により、携帯型電子装置の所有者が害を被ることを排

除でき、携帯型電子装置の所有者の財産または情報に関わるセキュリティを高める得る効果がある。

【００４５】（実施の形態３）次に、携帯型電子装置の所有者がその装置を盗まれたり紛失して、該携帯型電子装置を他人が拾得した場合に発生しうる問題は、元々の所有者はプライベイト情報や重要データを盗み見されたり、使用していない通話料金などの請求を請けるなど該携帯型電子装置の所有者が害を被る問題と、盗難や紛失した携帯型電子装置の所有者に送信した相手にとっても、不適切な状況であることを知らずに携帯型電子装置の所有者と思ってに送信したことで、送信相手または相手情報が害を被る問題がある。

【００４６】したがって、請求項３に対応する本実施の形態３では、携帯型電子装置の所有者が、その携帯型電子装置を盗まれたり紛失した場合は、図５に示すセキュリティを高める保全処理の制御ルーチンを実行する。ステップＳ１０において、携帯型電子装置の所有者は網管理局３６に対して変復調器（ＭＯＤＥＭ）を介しパソコン３２を用いて所有する携帯型電子装置に対して通信を開始すべく遠隔操作データを入力する。この場合に携帯型電子装置が携帯していない状況（盗難や紛失）および内部に記憶されている情報の重要度により送信する遠隔操作データの内容を選択する。遠隔操作データには制御コードが事前に付加されており、この制御コードは所有者のみが知っているキーワードある。

【００４７】そこで、電波通信手段を伝送媒体にしてデータ受信した遠隔操作データの識別結果により、携帯型電子装置の所有者に送信した相手または相手情報が害を被ることを排除する保全処理手段を備える携帯型電子装置において、送信した相手または相手情報が害を被るのを防止するための保全処理手段では、携帯型電子装置の所有者が予め記憶手段に記憶しておいたキーワードと、電波通信手段を媒体にし遠隔操作データを受信した時の識別結果のキーワード情報との一致を確認した後に、後述する実施の形態１５で説明する各保全処理を実行する。

【００４８】すなわち、遠隔操作データによって、

ａ．携帯型電子装置に送信した相手に、所有者が受信できない事情にある所定の情報を相手に送信する保全処理、

ｂ．携帯型電子装置に送信した相手からの受信情報を受信する機能を停止する保全処理、

ｃ．携帯型電子装置に送信した相手に、話中または使用中のデータを送信する保全処理、

ｄ．携帯型電子装置に送信した相手に、送信情報を送信する機能を停止する保全処理、

ｅ．携帯型電子装置に送信した相手に、所有者があらかじめ入力して記憶手段に蓄積記憶した紛失メッセイジを送信する保全処理、

ｆ．携帯型電子装置に送信した相手に、該携帯型電子装置の使用を防止する保全処理、のうち１つ以上の処理を実行する。

【００４９】したがって、本実施の形態３では、盗まれたり紛失した携帯型電子装置の所有者に送信した相手にとって、送信相手の携帯型電子装置が不適切な状況にあることを知り、保全処理することによって送信相手または相手情報が害をこうむるのを防止することができる。

【００５０】（実施の形態４）携帯型電子装置の所有者が、その携帯型電子装置を盗まれたり紛失した場合に、上記図５に示すセキュリティを高める保全処理の制御ルーチンのようにキーワードと遠隔操作データが所有者の手元にない所有者の携帯型電子装置に送信されると、該携帯型電子装置の保全処理手段は図６に示す遠隔操作データの処理ルーチンを実行する。以下、その処理ルーチンについて図６を参照して説明する。

【００５１】図６において、ステップＳ２０では、紛失の携帯型電子装置がキーワードと遠隔操作データを受信し、次のステップＳ２１において、遠隔操作のキーワードが予め所有者が記憶手段に記憶しておいたキーワードであるか否かを識別する。ここで、不一致である場合は保全処理システムを終了し、通常のモードに戻る。また、キーワードが一致した場合は保全処理システムを立ち上げ、装置のプロテクト機能を起動する。その後、遠隔操作データであるか否かを識別する。ここで、遠隔操作データでない場合は保全処理システムを終了し、通常のモードに戻る。また、遠隔操作データである場合はステップＳ２２に進み、遠隔操作データの保全内容を解析する。

【００５２】遠隔操作データは各保全処理にコードが予め定めてあり、例えば「警告発生」、「メッセイジ表示」、「所有者連絡発信」、「発信機能禁止」、「データ出力禁止」、「記憶データ消去」、「通信回線番号消滅」、「電源オフ」など、所定のコードにより分岐し、個々の保全処理ルーチンに進む。

【００５３】すなわち、ステップＳ２３では、遠隔操作データの内容が「警告発生」コードと一致すると判別した場合はステップＳ２４に進み、「警告発生」の保全処理を実行する。ステップＳ２３で不一致の場合は次の処理コードのステップＳ２５に進み、次々と一致するコードを検索して進む。その他の遠隔操作データの内容においても同様であり一致した場合には該当した保全処理を実行する。非該当のコードであれば保全処理システムを終了する又は固定の保全処理をする。

【００５４】次にステップ２５では、遠隔操作データの内容が「メッセイジ表示」コードと一致するか否かを識別し、一致した場合にはステップＳ２６に進み、「メッセイジ表示」の保全処理を実行する。ステップＳ２５で不一致の場合は次の処理コードのステップＳ２７に進む。ステップＳ２７では、遠隔操作データの内容が「発信機能禁止」コードと一致するか否かを識別し、一致し

た場合はステップＳ２８に進み、「発信機能禁止」の保全処理を実行する。ステップＳ２７で不一致の場合は次の処理コードのステップＳ２９に進む。

【００５５】ステップＳ２９では、遠隔操作データの内容が「所有者連絡発信」コードと一致するか否かを識別し、一致した場合はステップＳ３０に進み、「所有者連絡発信」の保全処理を実行する。ステップ２９で不一致の場合には次の処理コードのステップＳ３１に進む。

【００５６】次にステップＳ３１では、遠隔操作データの内容が「記憶データ消去」コードと一致するか否かを識別し、一致した場合にはステップＳ３２に進み、「記憶データ消去」の保全処理を実行する。ステップＳ３１で不一致の場合は次の処理コードのステップＳ３３に進む。ステップＳ３３では、遠隔操作データの内容が「データ出力禁止」コードと一致するか否かを識別し、一致した場合はステップＳ３４に進み、「データ出力禁止」の保全処理を実行する。ステップＳ３３で不一致の場合は次の処理コードのステップＳ３５に進む。

【００５７】ステップＳ３５では、遠隔操作データの内容が「通信回線番号消滅」コードと一致するか否かを識別し、一致した場合はステップＳ３６に進み、「通信回線番号消滅」の保全処理を実行する。ステップＳ３５で不一致の場合は次の処理コードのステップＳ３７に進む。ステップＳ３７では、遠隔操作データの内容が「記憶データ転送」コードと一致するか否かを識別し、一致した場合にはステップＳ３８に進み、「記憶データ転送」の保全処理を実行する。ステップＳ３７で不一致の場合は次の処理コードのステップＳ３９に進む。ステップＳ３９では、遠隔操作データの内容が「使用者の識別」コードと一致するか否かを識別し、一致した場合はステップＳ４０に進み、「使用者の識別」の保全処理を実行する。ステップＳ３９で不一致の場合は次の処理コードのステップＳ４１に進む。

【００５８】ステップＳ４１では、遠隔操作データの内容が「電源オフ」コードと一致するか否かを識別し、一致した場合はステップＳ４２に進み、「電源オフ」の保全処理を実行する。ステップＳ４１で不一致の場合は次の処理コードのステップＳ４３に進み、どのコードにも非該当のコードであれば、ステップＳ４５で保全処理システムを終了する。又はステップＳ４４で固定の保全処理として例えば「電源オフ」の保全処理を実行して終了する。

【００５９】上記の説明のように本実施の形態４では、、携帯型電子装置は携帯型電子装置の所有者が予め入力したキーワードを記憶手段に記憶しておき、電波通信手段を媒体にして遠隔操作データを受信し、その識別結果の保全処理コード情報を記録手段に記録し、この記憶手段のキーワードと保全処理コード情報との一致を確認した後で、図６に示す処理を実行することで、携帯型電子装置の保全を実現できるとともに、ケースバイケースで最適の保全処理を選択し、最適の運用を適用することができる効果がある。

【００６０】（実施の形態５）本発明の実施の形態５における保全処理手段の保全処理内容ａについて、図７を参照して説明する。

【００６１】保全処理内容ａは、盗難や紛失された携帯型電子装置を所有者以外の他人が使用しようとしても、携帯型電子装置の本来の機能を停止して他人が使用できなくする「電源オフ」の保全処理である。

【００６２】図７は携帯型電子装置の本来の機能を停止するための「電源オフ」の保全処理ルーチンを示すフローチャートである。まず、ステップＳ４４１において「電源オフ」フラッグがオンかを判定し、「電源オフ」フラッグがオンでない場合はステップＳ４４２に進み、「電源オフ」の保安処理を実行しない。また、「電源オフ」フラッグがオンである場合はステップＳ４４３に移行してパワーオンスイッチ・ディスエーブルフラッグをオンする。そして、ステップＳ４４４で携帯型電子装置の電源を強制的にオフし、「電源オフ」の保全処理を実施し（ステップＳ４４５）、電源オンを禁止する命令が優先的に実行される。

【００６３】このように、遠隔操作データで「電源オフ」保全処理をした場合、マニュアルモードにして携帯型電子装置の電源スイッチをオンしても、制御部はパワーオンシーケンスでフラッグがオンを確認し、電源をオフに移行させる。従って、携帯型電子装置の電源がオンにならないので、例え盗難に遭遇したような場合であっても他人に使用されず、回線使用料金が無謀に請求されることがない。

【００６４】この「電源オフ」保全処理は、携帯型電子装置の電源スイッチをオフにしてしまうもので、手順上極めて明解な保全処理であり、所有者が携帯型電子装置を盗まれたり紛失したことに気が付いた場合において、以下に示す保全処理内容ｂ～ｊなどで処理できなかった折に最終的に施す保全処理として活用するのに適している。更に他の保全処理内容ｂ～ｊなどで処理した後、「電源オフ」の保全処理を複合させて活用するようにしてもよい。

【００６５】また、「電源オフ」保全処理は、携帯型電子装置の本来の機能を停止することを目的にするもので、上記のパワーオンスイッチ・ディスエーブルフラッグをオンする以外の手段で、マイクロコンピュータのリセットオンや駆動用発振機能オフなどの手段などあらゆるハード手段も含むものである。

【００６６】多くの保全処理のうち１つ以上の処理を遠隔操作データで実施する結果により、例え携帯型電子装置が盗まれたり紛失しても、携帯型電子装置の個人データの保護や他人に使用されての所有者の害を被ることを排除する所定のセキュリティを高める効果がある。

【００６７】特に、本実施の形態５では、電源が入らな

いので装置の基本機能を殺す保全処理により、装置の紛失者にとって最小限度の損失に抑えることができる。

【００６８】（実施の形態６）本発明の実施の形態６における保全処理手段の保全処理内容ｂについて、図８を参照して説明する。

【００６９】保全処理内容ｂは、盗難や紛失された携帯型電子装置を所有者以外の他人が使用すると、視覚または聴覚によりアラームを発生して使用を禁止する「警告発生」の保全処理である。例えば、置き忘れや紛失された携帯型電子装置の表示部に所有者の住所と電話番号などの連絡先および拾得者へのメッセージなどを表示すること、またはスピーカから呼び掛けを音声を発信することにより、拾得者から所有者への返還を容易にする。

【００７０】図８は携帯型電子装置の本来の機能を停止するための「警告発生」の保全処理ルーチンを示すフローチャートである。「警告発生」の保全処理ルーチンでは、まず、ステップＳ２４１において「警告発生」フラッグがオンかを判定し、「警告発生」フラッグがオンでない場合はステップＳ２４２に進み、「警告発生」の保安処理を実行しない。また、「警告発生」フラッグがオンである場合はステップＳ２４３に移行してスピーカからアラーム音を発生させ、また液晶などの表示部の全面を点滅させる（ステップＳ２４４）。そして、アラーム音の発生時間及び表示部の表示時間をカウントし（ステップＳ２４５）、所定時間経過したかを判定する（ステップＳ２４６）。ここで、所定時間経過しない場合はステップＳ２４３に戻り、所定時間経過した場合はステップＳ２４１に戻る。

【００７１】このように、例え盗難や紛失に遭遇したような場合であっても他人がアラーム音を止めることがでず、表示部の点滅の繰り返し表示を止めることができない。したがって、紛失した場合に第３者に発見し拾得しやすく、拾得者が使用することを防止し所有者に返還させる。

【００７２】ただし、警告音や表示部の点滅の繰り返しは、携帯型電子装置の電池の消費電力が大きいため、第３者に発見されずに電池の消耗になる恐れがあるので、一定時間のみ駆動させる。

【００７３】他の保全処理のうち１つ以上の処理を遠隔操作データで実施する結果により、例え携帯型電子装置が盗まれたり紛失しても、携帯型電子装置の個人データの保護や他人に使用されての所有者の害を被ることを排除する所定のセキュリティを高める効果がある。

【００７４】特に、本実施の形態では、装置の拾得者に警告発生により装置の他人使用の禁止を訴える保全処理により、装置の紛失者にとって他人に使用されることを防止し、併せて所有者に返還させる効果が大きい。

【００７５】（実施の形態７）本発明の実施の形態７における保全処理手段の保全処理内容ｃについて、図９を参照して説明する。

【００７６】保全処理内容ｃは、盗難や紛失された携帯型電子装置を所有者以外の他人が使用すると、所有者が予め記憶手段に蓄積記憶した連絡先やメッセージを呼び掛け表示し、装置を回収する「メッセージ表示」の保全処理である。例えば、盗まれたり紛失した携帯型電子装置の所有者の住所と電話番号などの連絡先および拾得者へのメッセージなどを表示部に表示すること、またはスピーカーから呼び掛けをすることにより、拾得者が使用することを防止したり、所有者に返還させる。

【００７７】図９は携帯型電子装置の本来の機能を停止するための「メッセージ表示」保全処理のルーチンを示すフローチャートである。まず、ステップＳ２６１において「メッセージ表示」フラッグがオンかを判定し、「メッセージ表示」フラッグがオンでない場合はステップＳ２６２に進み、「メッセージ表示」の保安処理を実行しない。また、「メッセージ表示」フラッグがオンである場合はステップＳ２６３に移行してメッセージコード番号によりメッセージ内容を選択し、記憶した所定の表示内容１を表示部に表示する（ステップＳ２６４）。そして、記憶した所定の呼び掛け音１をスピーカから発生させ（ステップＳ２６４Ａ）、メッセージ表示の保全処理を実施する（ステップＳ２６７）。

【００７８】また、メッセージコード番号により別のメッセージ内容を選択した場合は、記憶した所定の表示内容２を表示部に表示する（ステップＳ２６５）。そして、記憶した所定の呼び掛け音２をスピーカから発生させ（ステップＳ２６５Ａ）、メッセージ表示の保全処理を実施する（ステップＳ２６７）。また、メッセージコード番号により更に別のメッセージ内容を選択した場合は、記憶した所定の表示内容３を表示部に表示する（ステップＳ２６６）。そして、記憶した所定の呼び掛け音３をスピーカから発生させ（ステップＳ２６６Ａ）、メッセージ表示の保全処理を実施する（ステップＳ２６７）。

【００７９】このように「メッセージ表示」の保全処理のルーチンでは、メッセージ表示フラッグをオンすると事前に記憶した所定の表示内容が液晶などの表示部に表示できるから、携帯型電子装置を所有者以外の他人が使用すると、所有者が予め入力して記憶手段に蓄積記憶した連絡先やメッセージが表示されることになる。

【００８０】この場合、「メッセージ表示」の保全処理はコード番号により複数の使い分けが可能である。例えばコード番号により「所有者連絡先」、「住所」、「電話番号」、「拾得者へお願い」、「拾得者へのお礼内容」など、所有者が盗難や紛失された場所や場合によってメッセージを使い分けができる。例えば「拾得者へお願い」の場合は『この装置を拾って頂いた方は、お手数ですが次にご連絡頂きますようにお願い致します。私は○○です。電話番号が○○です。よろしくお願い致します。』のメッセージ内容を表示しスピーカから呼び掛け

をする。また「拾得者へのお礼内容」の場合は『この装置を拾った方は、お手数ですが次にご連絡して下さい。謝礼に○○を差し上げます。電話番号が○○です。返却住所が○○です。』のメッセージ内容を表示しスピーカから呼び掛けをする。

【００８１】このように本実施の形態では、盗難や紛失された携帯型電子装置の所有者の住所と電話番号などの連絡先および拾得者へのメッセージなどを表示部に表示すること、またはスピーカから呼び掛けをすることにより、拾得者が所有者に連絡をすることができれば、所有者に返還させることができる。また、拾得者が使用するたびに返却要求のメッセージで訴えると、拾得者が使用することを回避させることができる。

【００８２】他の保全処理のうち１つ以上の処理を遠隔操作データで実施する結果により、例え携帯型電子装置が盗まれたり紛失しても、携帯型電子装置の個人データの保護や他人に使用されての所有者の害を被ることを排除する所定のセキュリティを高める効果がある。

【００８３】特に、本本実施の形態では、装置の拾得者にメッセージ表示により装置の返却を訴える保全処理により、装置の紛失者にとって他人に使用されることを防止し、所有者に返還できる効果がある。

【００８４】（実施の形態８）本発明の実施の形態８における保全処理手段の保全処理内容ｄについて、図１０を参照して説明する。

【００８５】保全処理内容ｄは、盗難や紛失された携帯型電子装置を所有者以外の他人が使用すると、本来の機能を停止し、所有者が予め入力して記憶手段に蓄積記憶した連絡先にのみ交信する「所有者連絡発信」の保全処理である。例えば、盗難や紛失された携帯型電子装置の所有者が予め契約した警備会社の連絡先を登録しておけば、拾得者が無断使用しようとしてダイヤルした場合にも、警備会社の連絡先にすべて交信する。

【００８６】図１０は携帯型電子装置の本来の機能を停止するための「所有者連絡発信」の保全処理ルーチンを示すフローチャートである。まず、ステップＳ３０１において「所有者連絡発信」フラッグがオンかを判定し、「所有者連絡発信」フラッグがオンでない場合はステップＳ３０２に進み、「所有者連絡発信」の保安処理を実行しない。また、「所有者連絡発信」フラッグがオンである場合はステップＳ３０３に移行して、予め設定した連絡先の内容を記憶手段から選択し、記憶した所定の連絡先１を表示部に表示する（ステップＳ３０４）。そして、記憶した所定の連絡先１に自動発信・接続し（ステップＳ３０４Ａ）、所有者連絡発信の保全処理を実施する（ステップＳ３０７）。

【００８７】また、別の連絡先内容を選択した場合は、記憶した所定の連絡先２を表示部に表示する（ステップＳ３０５）。そして、記憶した所定の連絡先２に自動発信・接続し（ステップＳ３０５Ａ）、所有者連絡発信の保全処理を実施する（ステップＳ３０７）。

【００８８】このように「所有者連絡発信」の保全処理のルーチンでは、所有者連絡発信フラッグをオンすると事前に記憶した所定の連絡先にのみ交信可能になる。すなわち、盗難や紛失された携帯型電子装置を所有者以外の他人が使用すると、所有者連絡発信フラッグのオンを確認し、所定の連絡先に優先的に交信が移行する。したがって、所有者が予め所有者自身を連絡先に登録した場合は、所有者は拾得者と必ず交信ができ、拾得者に直に返却の依頼ができる。また、この場合、拾得者は所有者以外への交信使用することができないから、盗難にあった場合でも第３者は使用することができず、回線使用料金が無謀に請求されることがない。

【００８９】他の保全処理のうち１つ以上の処理を遠隔操作データで実施する結果により、例え携帯型電子装置を盗難や紛失されても、携帯型電子装置の個人データの保護や他人に使用されての所有者の害を被ることを排除する所定のセキュリティを高める効果がある。

【００９０】特に、本実施の形態では、装置の拾得者の使用に対し所有者連絡発信により連絡が取れ装置の返却を訴える保全処理により、装置の紛失者にとって他人に使用されることを防止し、所有者に返還できる効果がある。

【００９１】（実施の形態９）本発明の実施の形態９における保全処理手段の保全処理内容ｅについて、図１１を参照して説明する。

【００９２】保全処理内容ｅは、盗難や紛失された携帯型電子装置の本来の機能のうちを所有者があらかじめ入力した機能を停止する「発信機能禁止」の保全処理である。装置の本来の機能のうち例えば、ダイヤル入力機能を停止することにより発信通話を禁止したり、記録機能のみを停止することにより所有者に関する個人情報だけをセキュリティ保護するなど部分的な機能のみを保全処理する。

【００９３】図１１は携帯型電子装置の本来の機能を停止するための「発信機能禁止」の保全処理ルーチンを示すフローチャートである。まず、ステップＳ２８１において「発信機能禁止」フラッグがオンかを判定し、「発信機能禁止」フラッグがオンでない場合はステップＳ２８２に進み、「発信機能禁止」の保安処理を実行しない。また、「発信機能禁止」フラッグがオンである場合はステップＳ２８３に移行して、発信要求コード番号を無効にする発信機能をオフし、発信機能禁止の保全処理を実施する（ステップＳ２８４）。

【００９４】このように「発信機能禁止」の保全処理ルーチンでは、発信機能禁止フラッグをオンすると発信通話を禁止する。すなわち、盗難や紛失された携帯型電子装置を所有者以外の他人が使用すると、発信機能禁止フラッグがオンを確認し、発信通話の禁止へ優先的に移行する。したがって、拾得者は発信通話ができず他人への

交信使用することができず、盗難に遭遇した場合でも第３者に使用されることがなく、回線使用料金が所有者に無謀に請求されることがない。

【００９５】他の保全処理のうち１つ以上の処理を遠隔操作データで実施する結果により、例え携帯型電子装置を盗難や紛失されても、携帯型電子装置の個人データの保護や他人に使用されての所有者の害を被ることを排除する所定のセキュリティを高める効果がある。

【００９６】特に、本実施の形態では、装置の拾得者の使用に対し発信機能禁止の保全処理により、装置の紛失者にとって他人に使用されることを防止し、不当な使用に伴う料金が生じることを回避できる効果がある。

【００９７】（実施の形態１０）本発明の実施の形態１０における保全処理手段の保全処理内容ｆについて、図１２を参照して説明する。

【００９８】保全処理内容ｆは、盗難や紛失された携帯型電子装置の記録手段からデータの出力を禁止する「データ出力禁止」の保全処理である。例えば、携帯型電子装置の所有者に関する個人情報や内部機密データを特定な記憶指定ロックで保管し、予め指定したキーワード以外の手順では開示できないようにする。

【００９９】図１２は携帯型電子装置の本来の機能を停止するための「データ出力禁止」保全処理のルーチンを示すフローチャートである。まず、ステップＳ３４１において「データ出力禁止」フラッグがオンかを判定し、「データ出力禁止」フラッグがオンでない場合はステップＳ３４２に進み、「データ出力禁止」の保安処理を実行しない。また、「データ出力禁止」フラッグがオンである場合はステップＳ３４３に移行して、発信要求コード番号を無効にする発信機能のオフ内容を選択し、データ出力禁止の保全処理を実施する（ステップＳ３４４）。

【０１００】このように「データ出力禁止」の保全処理ルーチンでは、データ出力禁止フラッグをオンするとデータ出力を禁止する。すなわち、盗難や紛失された携帯型電子装置を所有者以外の他人が使用すると、データ出力禁止フラッグがオンを確認し、データ出力を禁止する処理に優先的に移行する。したがって、拾得者や第３者はデータを出力できず、所有者のデータや個人情報を所有者以外の他人が覗いたり利用することができない。また、盗難や紛失された後「データ出力禁止」の保全処理された携帯型電子装置は所有者以外の他人にとっては全くの単なる無機物にすぎなく、所有者の損失は携帯型電子装置のハードだけで、所有者の財産または情報に関わるセキュリティを高めることができる。

【０１０１】他の保全処理のうち１つ以上の処理を遠隔操作データで実施する結果により、例え携帯型電子装置を盗難や紛失されても、携帯型電子装置の個人データの保護や他人に使用されての所有者の害を被ることを排除する所定のセキュリティを高める効果がある。

【０１０２】特に、本実施の形態では、装置の内部の個人データや情報を保護するデータ出力禁止の保全処理により、装置の紛失者にとって他人に使用されることを防止し、不当な使用に伴う料金が生じることを回避できる効果がある。

【０１０３】（実施の形態１１）本発明の実施の形態１１における保全処理手段の保全処理内容ｇについて、図１３を参照して説明する。

【０１０４】保全処理内容ｇは、盗難や紛失された携帯型電子装置の記録手段のデータを消却し、他人に見られたり使用されないようにする「記憶データ消去」の保全処理であり、携帯型電子装置の記録部の所有者に関する個人情報やデータを消去し、他人の開示を回避する。

【０１０５】図１３は携帯型電子装置の本来の機能を停止するための「記憶データ消去」の保全処理ルーチンを示すフローチャートである。まず、ステップＳ３２１において「記憶データ消去」フラッグがオンかを判定し、「記憶データ消去」フラッグがオンでない場合はステップＳ３２２に進み、「記憶データ消去」の保安処理を実行しない。また、「記憶データ消去」フラッグがオンである場合はステップＳ３２３に移行して、記憶手段の所定のエリアのデータを消去し、記憶手段のユーザーエリアのデータ（個人情報、装置の固有情報、通話番号等）の選択を禁止する。その後、記憶データ消去の保全処理を実施する（ステップＳ３２４）。

【０１０６】このように「記憶データ消去」の保全処理ルーチンでは、記憶データ消去フラッグをオンすると記憶データが消去される。すなわち、盗難や紛失された携帯型電子装置を所有者以外の他人が使用すると、記憶データ消去フラッグがオンを確認し、記憶データを消去する処理に優先的に移行する。したがって、拾得者や第３者が盗難や紛失された携帯型電子装置を使用としても記憶データ消去されており、所有者のデータや個人情報を所有者以外の他人が覗いたり利用することができない。また、盗難や紛失された後「記憶データ消去」の保全処理された携帯型電子装置は所有者以外の他人にとっては全くの単なる無機物にすぎず、所有者の損失は携帯型電子装置のハードだけで、所有者の財産または情報に関わるセキュリティを高めることができる。

【０１０７】他の保全処理のうち１つ以上の処理を遠隔操作データで実施する結果により、例え携帯型電子装置を盗難や紛失されても、携帯型電子装置の個人データの保護や他人に使用されての所有者の害を被ることを排除する所定のセキュリティを高める効果がある。

【０１０８】特に、本実施の形態では、装置の内部の個人データや情報を保護する記憶データ消去の保全処理で、装置の紛失者にとって他人に使用されることを防止し不当な使用に伴う料金が生じることを回避し、個人データや情報を他人に悪用されることを阻止できる効果がある。

【０１０９】（実施の形態１２）本発明の実施の形態１２における保全処理手段の保全処理内容ｈについて、図１４を参照して説明する。

【０１１０】保全処理内容ｈは、盗難や紛失された携帯型電子装置の通信回線番号を消滅し、他人が使用できなくする「通信回線番号消滅」の保全処理であり、他人に悪用され通話料金の請求を回避する。

【０１１１】図１４は携帯型電子装置の本来の機能を停止するための「通信回線番号消滅」の保全処理ルーチンを示すフローチャートである。まず、ステップＳ３６１において「通信回線番号消滅」フラッグがオンかを判定し、「通信回線番号消滅」フラッグがオンでない場合はステップＳ３６２に進み、「通信回線番号消滅」の保安処理を実行しない。また、「通信回線番号消滅」フラッグがオンである場合はステップＳ３６３に移行して、通信ダイヤルスイッチディスエーブルフラッグをオンする。そして、ステップＳ３６４で携帯型電子装置の電源を強制的にオフし、通信回線番号消滅の保全処理を実施する（ステップＳ３６５）。

【０１１２】このような「通信回線番号消滅」の保全処理ルーチンでは、通信回線番号消滅フラッグをオンすると記憶された携帯型電子装置の通信回線番号を消滅される。すなわち、盗難や紛失された携帯型電子装置を所有者以外の他人が使用すると、通信回線番号消滅フラッグがオンを確認し、携帯型電子装置に記憶された通信回線番号を消去する処理に優先的に移行する。したがって、拾得者や第３者が盗難や紛失された携帯型電子装置を使用としても記憶されていなければならない通信回線番号が消滅され、他人が全く利用することができない。また、盗難や紛失された後「通信回線番号消滅」の保全処理された携帯型電子装置は所有者以外の他人にとっては全くの単なる無機物にすぎなく、所有者の損失は携帯型電子装置のハードだけで、所有者の財産または情報に関わるセキュリティを高めることができる。また、通信回線番号は、携帯型電子装置の製造者または販売者のみが特殊な方法で入力することができ、電源をオフしても登録内容が保持される内部記憶媒体部に１度だけ記憶された各装置の固有の番号である。

【０１１３】他の保全処理のうち１つ以上の処理を遠隔操作データで実施する結果により、例え携帯型電子装置が盗まらたり紛失しても、携帯型電子装置の個人データの保護や他人に使用されることによる所有者が害を被ることを排除する所定のセキュリティを高める効果がある。

【０１１４】特に、本実施の形態では、装置の拾得者の使用に対し通信回線番号を消滅させて発信機能を不可能にする保全処理であるから、装置の紛失者にとって他人に使用されることを防止し、不当な使用に伴う料金が生じることを回避できる　果がある。

【０１１５】（実施の形態１３）本発明の実施の形態１３における保全処理手段の保全処理内容ｉについて、図１５を参照して説明する。

【０１１６】保全処理内容ｉは、盗難や紛失された携帯型電子装置の記録手段のデータを他の所定の電子装置に転送し、記憶データを回収する「記憶データ転送」の保全処理であり、携帯型電子装置の記録部の所有者に関する個人情報やデータを他の所定の電子装置に転送し、その後、該装置の記録部の個人情報やデータを他の所定の電子装置が流用する。

【０１１７】図１５は携帯型電子装置の本来の機能を停止するための「記憶データ転送」の保全処理ルーチンを示すフローチャートである。まず、ステップＳ３８１において「記憶データ転送」フラッグがオンかを判定し、「記憶データ転送」フラッグがオンでない場合はステップＳ３８２に進み、「記憶データ転送」の保安処理を実行しない。また、「記憶データ転送」フラッグがオンである場合はステップＳ３８３に移行して記憶手段から記憶データを読み出し、記憶データを送信する（ステップＳ３８４）。その後、データ転送が完了したかを判定する（ステップＳ３８５）。ここで、データ転送が完了しない場合はステップＳ３８３に戻り、データ転送が完了した場合はステップＳ３８６に移行して記憶部を破壊しデータを消去する。そして、記憶データ転送の保全処置を実施する（ステップＳ３８７）。

【０１１８】このように「記憶データ転送」の保全処理ルーチンでは、記憶データ転送フラッグをオンすると記憶データを転送し回収される。これにより、盗難や紛失された携帯型電子装置に記憶させた個人情報やデータを読み取り転送させることができ、更にその後装置の記録手段の記憶データを消去する処理に優先的に移行する。したがって、携帯型電子装置を盗難や紛失された時に本保全処理により、所有者は他の所定の電子装置に記憶データを読み取り転送し回収でき、その後で元の記憶データを消去できるため、拾得者や第３者が盗難や紛失された携帯型電子装置を使用としても記憶データは消去されており、所有者のデータや個人情報を所有者以外の他人が覗いたり利用することができない。

【０１１９】他の保全処理のうち１つ以上の処理を遠隔操作データで実施する結果により、例え携帯型電子装置が盗まれたり紛失しても、携帯型電子装置の個人データの保護や他人に使用されることによる所有者が害を被ることを排除する所定のセキュリティを高める効果がある。

【０１２０】特に、本実施の形態では、装置の内部の個人データや情報を遠隔操作で転送する「記憶データ転送」の保全処理により、装置の紛失者にとって他人に使用される前に内部の個人データや情報を転送回収して、その後装置内部の記憶データを消去し、装置の紛失者にとって他人に使用されることを防止し、不当な使用に伴う料金が生じることを回避できる効果がある。

【０１２１】（実施の形態１４）本発明の実施の形態１４における保全処理手段の保全処理内容ｊについて、図１６を参照して説明する。

【０１２２】保全処理内容ｉは、使用者を識別し、所有者以外の他人が携帯型電子装置を使用を不可能にする「使用者の識別」の保全処理である。使用者の識別は、例えばパスワード入力、指紋認識、声紋認識など使用者の識別手段により、所有者以外の人が携帯型電子装置を使用した時に保全処理が実行される。

【０１２３】図１６は携帯型電子装置の本来の機能を停止するための「使用者の識別」の保全処理ルーチンを示すフローチャートである。まず、ステップＳ４０１において「使用者の識別」フラッグがオンかを判定し、「使用者の識別」フラッグがオンでない場合はステップＳ４０２に進み、「使用者の識別」の保安処理を実行しない。また、「使用者の識別」フラッグがオンである場合はステップＳ４０３に移行して装置の発信通話機能を先ずオフし、次いで使用者識別番号かを判定する（ステップＳ４０４）。ここで、使用者識別番号でない場合はステップＳ４０２に戻り、使用者識別番号の場合はステップＳ４０５、ステップＳ４０６、ステップＳ４０７のいずれかへ移行して使用者の識別を行う。

【０１２４】使用者の識別の一つは、使用時にパスワードの入力を要求し、この入力パスワードと携帯型電子装置の所有者が予め設定し登録したパスワードと比較し（ステップＳ４０５）、パスワードが一致したかを判定する（ステップＳ４０５Ａ）。ここで、一致した場合はステップＳ４０９に移行して正常使用を可能にする。また、不一致の場合は、パスワードの誤入力に対するリトライ回数を３回に定め（ステップＳ４０５Ｂ）、パスワードの誤入力が３回以上あった場合は更に強度の保全処理を実行する（ステップＳ４０８）。この時の所有者が予め設定するパスワードは、電源をオフしても登録内容が保持される記憶部に１度だけ記憶する。使用前にパスワードの入力してから運用する保全処理は従来もあったが、通常時には厄介なこともあり平常はその保全処理を解除していることが多い。しかし本保全処理は、携帯型電子装置の所有者が、その携帯型電子装置が盗まれたり紛失した場合に、保全を要する携帯型電子装置に遠隔操作データを送信し、パスワードによる保全処理の機能を働かさせるところに特徴を有する。

【０１２５】また、使用者の識別の他の例としては、携帯型電子装置を使用する者に指紋の入力を要求し、この指紋と携帯型電子装置の所有者が予め設定し登録した指紋とを比較し（ステップＳ４０６）、指紋が一致したかを識別する（ステップＳ４０６Ａ）。ここで、使用者の指紋入力する場合は、例えば携帯電話機を持つ手の親指が当たる部分に指紋を検出する機能と指紋を認識する機能を付加することで可能になる。したがって、指紋の一致が認識された場合はステップＳ４０９に移行して正常使用を可能にする。また、指紋の不一致が認識された場合は、指紋の誤入力に対するリトライ回数を３回に定め（ステップＳ４０６Ｂ）、指紋の誤入力が３回以上あった場合は更に強度の保全処理を実行する（ステップＳ４０８）。

【０１２６】また、使用者の識別の更に他の例としては、パスワードを音声化し、予め登録したパスワードの音声データ（声紋）とマイクから入力した声紋を照合し（ステップＳ４０７）、声紋が一致したかを認識する（ステップＳ４０７Ａ）。ここで声紋の一致が認識された場合はステップＳ４０９に移行して正常使用を可能にする。また、声紋の不一致が認識された場合は、声紋の誤入力に対するリトライ回数を３回に定め（ステップＳ４０７Ｂ）、声紋の誤入力が３回以上あった場合は更に強度の保全処理を実行する（ステップＳ４０８）。

【０１２７】このように「使用者の識別」の保全処理ルーチンでは、使用者の識別フラッグをオンすると使用者の識別手段によりパスワード、指紋、声紋を識別し、所有者以外の人が携帯型電子装置を使用を検出した場合には使用者の識別フラッグがオンを確認し、装置の発信通話を禁止する処理に優先的に移行する。したがって、拾得者は発信通話ができず他人への交信使用することができない。

【０１２８】他の保全処理のうち１つ以上の処理を遠隔操作データで実施する結果により、例え携帯型電子装置を盗難や紛失されても、携帯型電子装置の個人データの保護や他人に使用されることを排除する所定のセキュリティを高める効果がある。

【０１２９】（実施の形態１５）次に、本発明の請求項１５に対応する実施の形態１５の保全処理について説明する。この実施の形態による保全処理内容は、次に示す内容から構成される。

【０１３０】保全処理内容ａは、携帯型電子装置に送信した相手に、所有者が受信できない事情にある所定の情報を相手に送信する保全処理であり、送信した相手に、個人情報やデータを所有者が受信できない事情にある旨を知らせ、送信することを未然に回避させることで、他人の拾得者に個人情報やデータが漏洩されることを保全する。

【０１３１】保全処理内容ｂは、携帯型電子装置に送信した相手からの受信情報を受信する機能を停止する保全処理であり、他人の拾得者に個人情報やデータが漏洩されないように、相手からの受信情報を受信する機能を停止し保全する。

【０１３２】保全処理内容内容ｃは、携帯型電子装置に送信した相手に、話中または使用中のデータを送信する保全処理であり、送信した相手が、個人情報やデータを所有者に送信する前に話中または使用中の信号データを一方的に送信して、送信することを未然に回避させることで、他人の拾得者に個人情報やデータが漏洩されるこ

とを保全する。

【０１３３】保全処理内容ｄは、携帯型電子装置に送信した相手に、送信情報を送信する機能を停止する保全処理であり、送信した相手が、個人情報やデータを所有者に送信する前に通信手続きの動作において、例えばアクセス信号を送信せずに、送信情報を送信する機能を停止し、交信を回避する。

【０１３４】保全処理内容ｅは、携帯型電子装置に送信した相手に、所有者が予め入力して記憶手段に蓄積記憶した紛失メッセイジを送信する保全処理であり、保全処理内容ｃにおける話中または使用中の信号データの代わりに、予め入力して記憶手段に蓄積記憶した紛失メッセージを一方的に送信して、送信することを未然に回避させることで、他人の拾得者に個人情報やデータが漏洩されることを保全する。

【０１３５】保全処理内容ｆは、携帯型電子装置に送信した相手に、該携帯型電子装置の使用を防止する保全処理であり、他人の拾得者が拾得した携帯型電子装置を使用した個人情報やデータを、所有者の個人情報やデータとして相手が交信したことによる問題を回避するために、転送先を固定し記憶された住所など消去するもので、他人の開示を回避する。

【０１３６】以上の保全処理のうち１つ以上の処理を実施する結果により、例え携帯型電子装置を盗まれたり紛失しても、その装置の所有者に送信した相手にとって、携帯型電子装置の個人データの保護や他人に使用されて所有者が害を被ることが排除され、所定のセキュリティを高めることができる。

【０１３７】（実施の形態１６）次に、本発明の請求項１６に対応する実施の形態１６の保全処理について説明する。この実施の形態は、電波通信手段を伝送媒体とし、所有者が予め入力して記憶手段に蓄積記憶したキーワード信号を受信した場合に、遠隔操作データの識別結果により、強制的に携帯型電子装置の保全機能を駆動し、所有者が害を被ることを排除する所定のセキュリティを高める保全処理手段を設けたところにある。

【０１３８】図１において、携帯型電子装置１を盗まれたり紛失した所有者は、一般公衆電話や携帯電話としてのＰＨＳなど電話機３を操作して携帯型電子装置１に電話をかける。この場合市内や市外の一般公衆電話３Ａから公衆回線網２ｃを介して、またＰＨＳデータ通信装置や携帯電話としてのＰＨＳ３から無線通信回線２ｂを介して保全を要する携帯型電子装置１に遠隔操作データを送信する。

【０１３９】次に、本実施形態の保全処理動作について図１７に示す保全確認のルーチンを用いて説明する。

【０１４０】盗難や紛失した携帯型電子装置１は、多くの場合に他人が拾得していることがあり、通話が可能である。次に携帯型電子装置１を盗まられたり紛失した所有者は、所有者が予め入力して記憶手段に蓄積記憶したキーワード信号を送信する。記憶手段に蓄積記憶したキーワード信号を受信した場合に、該携帯型電子装置１は遠隔操作データを受信する受信部１１で受信し（ステップＳ１７１）、受信した遠隔操作データが予め記憶された所定のキーワード信号と一致することを識別する識別部１２で判定する（ステップＳ１７２）。識別部１２の識別結果により一致が確認された場合のみ保全確認信号を発信する（ステップＳ１７３）。この保全確認信号の指示により他の機能を強制的にオフし（ステップＳ１７４）、次いで保全部１３が強制的に携帯型電子装置の保全機能を駆動し（ステップＳ１７５）、携帯型電子装置の所有者が害を被ることを排除する所定の保全処理をするように動作する。

【０１４１】特に、本実施の形態では、装置の紛失者が予め入力して記憶手段に蓄積記憶したキーワード信号を送信し、強制的に携帯型電子装置の保全機能を駆動し、装置の紛失者にとって他人に使用されることを防止できる。

【０１４２】（実施の形態１７）次に、請求項１７に対応する実施の形態１７について、図１８を参照して説明する。この実施の形態では、所有者が予め入力して記憶手段に蓄積記憶した呼び出し信号回数のパターンを受信した場合に、遠隔操作データの識別結果により、強制的に携帯型電子装置の接続を行い、所有者が害を被ることを排除する所定のセキュリティを高める保全処理手段を設けたものである。

【０１４３】すなわち、第１回目の受信の呼び出し信号回数をカウントし（ステップＳ１０１）、そのカウント値が予め設定した第１回目のコール回数と識別したかを判定する（ステップＳ１８２）。ここで、否定判定された場合はステップＳ１８１に戻り、肯定判定された場合はステップＳ１８３に進む。ステップＳ１８３では、第２回目の受信の呼び出し信号回数をカウントし、そのカウント値が予め設定した第２回目のコール回数と識別したかを判定する（ステップＳ１８４）。ここで、否定判定された場合はステップＳ１８１に戻り、肯定判定された場合はステップＳ１８５に進む。

【０１４４】ステップＳ１８５では、第３回目の受信の呼び出し信号回数をカウントし、そのカウント値が予め設定した第３回目のコール回数と識別したかを判定する（ステップＳ１８６）。ここで、否定判定された場合はステップＳ１８１に戻り、肯定判定された場合はステップＳ１８７に進む。ステップＳ１８７では保全システムを立ち上げ、次の受信の呼び出し信号回数から保全内容を識別したかを判定する（ステップＳ１８８）。保全内容を識別した場合はステップＳ１８９に進み、遠隔操作データの保全内容を解析する。そして、遠隔操作データの識別結果に応じた保全処理を実施する（ステップＳ１９０）。

【０１４５】このように盗難や紛失した携帯型電子装置

を拾得した者が応答したとか、交信ができない事態の場合においても、予め入力して記憶手段に蓄積記憶した呼び出し信号回数のパターンを受信した場合に、遠隔操作データの識別結果により強制に電源供給を中断し、即停止するなどの所定の保全処理内容を適用するように動作する。

【０１４６】上記の呼び出し信号回数のパターンは、例えば第１回目の１０回呼び出し後一旦フック回線をオフし、第２回目の５回呼び出し後一旦フック回線をオフし、第３回目の８回呼び出し後一旦フック回線をオフするものであり、この呼び出し信号回数のパターンを所定時間の期間に繰り返すパターンを受信した場合に、所定の保全処理内容を適用する。

【０１４７】なお、本発明の請求項８は、実施の形態４における携帯型電子装置の遠隔操作データの処理ルーチンで、図６のステップＳ２０、ステップＳ２１によるキーワード識別に相当する遠隔操作か否かを識別する方法を代替えするものである。その結果により個々の保全処理の内容については、上記と同様のため説明を省略する。

【０１４８】本実施の形態による保全処理は、携帯型電子装置を情報携帯端末電話装置に適用した実例であるが、一般的な情報携帯端末機やＰＨＳやコードレス電話機においても適用できるものである。

【０１４９】特に、本実施の形態では、装置の拾得者が応答しなとか、交信ができない事態の場合においても、呼び出し信号回数のパターンによる遠隔保全処理を起動させ、装置の紛失者にとって他人に使用されることを防止できる。

【０１５０】（実施の形態１８）次に、本発明の請求項１８に相当する実施の形態１８の携帯型電子装置保全システムについて図１９を参照しながら説明する。

【０１５１】この実施の形態では、携帯型電子装置を紛失または置き忘れを防止するための携帯型電子装置保全システムである。特に微弱電波或いは超音波などを用いた子機を備えた携帯型電子装置に関するもので、実施の形態１のように、この種の携帯型電子装置はいつか如何なる時でも遺失の件数は膨大し、小型携帯上は優れており便利であるが盗難に合いやすい。これらの遺失対策はそれらの所有者が細心の注意を払う以外にないが、それが如何に効果の少ない方法であるかを多く体験していることである。

【０１５２】この問題を解決する手段として本実施の形態では、微弱電波或いは超音波或いは誘導電波などを発振する発振手段と、それを本体に送信する微弱電力送信手段を有する子機を備え、該子機からの保全処理を促すための発振データを受信する手段、受信した操作データを識別する手段、該識別の結果により携帯型電子装置の所有者が害を被ることを排除する所定の保全手段を備えてた携帯型電子装置（本体）で構成し、上記微弱電力送信手段を有する子機は、鎖付きのペンダントやピアスのように身近に携帯する小型軽量が望まれる。子機は、服装のポケットなどにしっかりと挿入できるようにフックやベルト付きにし、またはピアスやペンダントに内蔵し子機自身の紛失を防ぐものである。

【０１５３】本体の携帯型電子装置は子機からの保全処理を促すための発振データを受信する受信手段を有し、該受信した操作データを識別する手段で、所定の保全手段を動作するものである。また前記微弱電力送信手段の送信する信号が該受信手段に着信する距離を例えば数メートル程となるように設定し、その通信可能距離以上に上記送受信手段、すなわち本体と子機との両者が離れると着信信号レベルが所定以下になり、該受信した操作データを識別する手段は、本体の携帯型電子装置が所定の距離以上に所有者から離れた、即ち所有者が本体の携帯型電子装置を置き忘れたか遺失したものと識別する。そして該識別の結果により携帯型電子装置の所有者が害を被ることを排除する所定の保全手段を動作させる。保全手段は、例えば所有者にその旨を気付かせるように警告する警告ブザーを鳴らすことや、携帯型電子装置本体に保全処理を促すための前記実施の形態１のように各種の保全機能を起動させる。

【０１５４】図１９は、本実施の形態１８の一例を示す構成図である。同図でにおいて、子機における発振器２１からの出力信号を伝送部２２で変調増幅し、微弱電力送信手段２３からアンテナを通して所定の微弱電力信号を送信する。

【０１５５】一方、該信号を本体のアンテナから微弱電力受信部２４で受信する。受信信号は伝送部２５で復調増幅され、検波部２６により検波した後、その受信レベルが予め設定したレベル以下かどうかを判定部２７で判別し、受信のレベルによって子機と本体との空間距離が所定の距離以上かどうかを判別する。子機と本体との空間間距離が所定の距離に比べて離れると本体に保全処理を促すための各種の保全処理を行う保全手段２８が動作し、例えば所有者にその旨を気付かせるように警告ブザーを鳴らす。

【０１５６】上記のように、所有者が携帯型電子装置を紛失または置き忘れそうになった場合に、本システムが作動して未然に紛失または置き忘れを防止し回避することができる。また所有者が携帯型電子装置を紛失または置き忘れてしまった場合でも、自動的に本体に保全処理を促すための各種の保全機能を起動させるため、他人に拾得されても装置の所有者の財産または情報に関わるセキュリティを高めることが簡単に実施できる。

【０１５７】（実施の形態１９）図２０は、本発明の請求項１９に対応する実施の形態１９の構成を示す機能ブロック図である。同図において、子機は発振器４１、発振器４１からの出力信号を変調増幅する伝送部４２、伝送部４２からの信号を本体へ送信するとともに本体から

の信号を受信する微弱電力伝送手段４３、微弱電力伝送手段４３の受信信号を復調増幅する伝送部４４、復調信号を検波する検波部４５、検波信号の受信レベルが予め設定したレベル以下かどうかを判別し、かつ受信レベルによって子機と本体との空間距離が所定の距離以上かどうかを判別する判定部４６、子機保全のための各種の保全処理を行う保全手段４７、信号の交信をリセットするリセット部４８から構成されている。

【０１５８】また、本体は子機からの信号を受信するとともに子機へ進行を送信する微弱電力伝送手段４９、微弱電力伝送手段４９の受信信号を復調増幅する伝送部５０、復調信号を検波する検波部５１、検波信号の受信レベルが予め設定したレベル以下かどうかを判別し、かつ受信レベルによって子機と本体との空間距離が所定の距離以上かどうかを判別する判定部５２、本体保全のための各種の保全処理を行う保全手段５３、信号の交信をリセットするリセット部５４、発振器５５、発振器５５からの出力信号を変調増幅して微弱電力伝送手段４９へ出力する伝送部５６から構成されている。

【０１５９】この構成において、図１９に示し場合と同様に形態型電子装置の本体と子機間の距離が、例えば数メートル程度離れることで通信可能距離以上になると着信信号レベルが所定以下になり、該受信した操作データを識別する判定部４６及び５２は、本体の携帯型電子装置が所定の距離以上に所有者から離れた、即ち所有者が本体の携帯型電子装置を盗難および置き忘れたか遺失したものと識別すると、その識別結果により携帯型電子装置の所有者が害を被ることを排除する所定の保全手段４７及び５３が動作を開始し、未然に盗難および紛失または置き忘れを防止し回避することができる。保全手段４７及び５３は、例えば所有者にその旨を気付かせるように警告する本体及び子機の一方または双方で警告ブザーを鳴らすことや、携帯型電子装置本体に保全処理を促すための前記実施の形態のように各種の保全機能を起動させる。

【０１６０】このように本体及び子機に警告を発生する手段を有することによって、所有者が携帯型電子装置を盗難および紛失または置き忘れそうになった場合に、本システムの保全手段が作動して未然に盗難および紛失または置き忘れを防止し回避することができる。特に盗難および置き引きに遭遇した場合に、警告音を発生することの効果や危険性を考慮し、子機から警告音を発生させずバイブレータ振動で所有者に報知することで周囲の人々に気付かれないで紛失または置き忘れを回避できる。また、警告音を発生させて周囲の人々に気付かせたいのか、または周囲の人々に気付かれないで解決するか切り替えることができる。

【０１６１】更に、子機に着信信号レベルを換算し本体と子機との両者間の距離を表示する機能を設ける携帯型電子装置においては、所有者が携帯型電子装置を紛失または置き忘れそうになった場合に、本体と子機との両者間の距離を表示する子機により、本体の存在する位置を検索することができる。例えば部屋内で本体を見失った場合に、子機と本体間の距離の表示の変化で本体が存在する位置を見つけ出すことが可能になる。

【０１６２】また、上記の本実施の形態において、信号の交信をリセットするリセット部を付加することが運用上便利である。リセット部を付加することは、所有者が携帯型電子装置を紛失または置き忘れそうになった場合に動作した後、再度本実施例の機能を運用させる上で極めて大きい効果を有する。

【０１６３】上記の説明により本発明のように携帯型電子装置を紛失または置き忘れを防止するための携帯型電子装置の保全システムを容易に実施することができ、携帯型電子装置を紛失または置き忘れを防止する上で大きな効果を有する。

【０１６４】なお、上記実施の形態における保全処理は携帯型電子装置を情報携帯端末電話装置に適用した場合について説明したが、一般的な情報携帯端末機やＰＨＳやコードレス電話機においても適用できるものである。

【０１６５】

【発明の効果】以上のように本発明の携帯型電子装置の保全システムによれば、上記実施例より明らかなように、以下の効果を得ることができる。

【０１６６】携帯型電子装置（ＰＨＳ、携帯電話機も含む電波通信手段を有するデータ処理端末装置）の盗難や紛失に対して、その所有者が遠隔操作するとこにより、携帯型電子装置の所有者が害を被ることを排除する所定の保全手段が動作し、携帯型電子装置の所有者の財産または情報に関わるセキュリティを高めることができる。すなわち、簡単に携帯型電子装置の内部のデータを保護することができ、更に他人に使用されても料金を支払うという不具合を回避することができる。

【０１６７】また、所有者が携帯型電子装置の盗難や紛失に気が付いた場合に、所有者が積極的に保全を要求することにより、携帯型電子装置の所有者に不利益となる要因を防止することができる。即ち、携帯型電子装置の記憶内部および仕様に関してプロテクトをかけて保護することができる。

【０１６８】また、盗難や紛失した携帯型電子装置の所有者に送信した相手にとっても、不適切な状況であることを知らずに携帯型電子装置の所有者と思ってに送信したことで、送信相手または相手情報が害を被る問題が発生するという不具合を回避することができる。即ち、盗難や紛失した携帯型電子装置の所有者や送信相手者が害を被ることを排除することができる。

【０１６９】また、本発明の携帯型電子装置の保全システムによれば、所有者が携帯型電子装置を紛失または置き忘れそうになった場合に、本システムが作動して未然に紛失または置き忘れを防止し回避することができるほ

か、所有者が携帯型電子装置を紛失または置き忘れてしまった場合でも、自動的に本体に保全処理を促すための各種の保全機能を起動させるため、他人に拾得されても装置の所有者の財産または情報に関わるセキュリティを高めることが簡単に実施できる。

【図面の簡単な説明】

【図１】本発明の実施の形態１における携帯型電子装置の保全システムの概略構成図

【図２】本発明の実施の形態２における携帯型電子装置の保全システムの構成を示す機能ブロック図

【図３】本発明の実施の形態２におけるプロトコールのハードウェア構成図

【図４】本発明における携帯型電子装置のネットワークシステムを示す図

【図５】本発明におけるセキュリティを高める保全処理の制御ルーチン図

【図６】本発明における遠隔操作データの処理ルーチン図

【図７】本発明における電源オフの保全処理ルーチンを示すフローチャート

【図８】本発明における警告発生の保全処理ルーチンを示すフローチャート

【図９】本発明におけるメッセイジ表示の保全処理ルーチンを示すフローチャート

【図１０】本発明における所有者連絡発信の保全処理ルーチンを示すフローチャート

【図１１】本発明における発信機能禁止の保全処理ルーチンを示すフローチャート

【図１２】本発明におけるデータ出力禁止の保全処理ルーチンを示すフローチャート

【図１３】本発明におけるデータ出力消去の保全処理ルーチンを示すフローチャート

【図１４】本発明における通信回線番号消滅の保全処理ルーチンを示すフローチャート

【図１５】本発明における記憶データ転送の保全処理ルーチンを示すフローチャート

【図１６】本発明における使用者の識別の保全処理ルーチンを示すフローチャート

【図１７】本発明における保全確認のルーチンを示すフローチャート

【図１８】本発明における呼び出し信号による遠隔操作の処理のルーチンを示すフローチャート

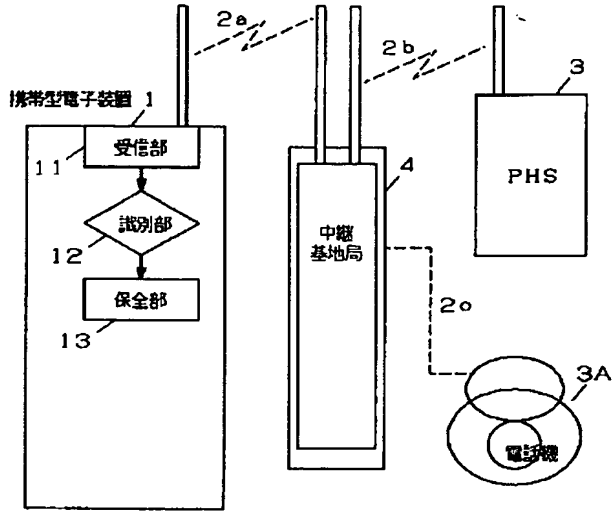
【図１９】本発明の実施の形態１８による携帯型電子装＊置の保全システムを示す構成図

＊【図２０】本発明の実施の形態１９による携帯型電子装置の保全システムを示す構成図

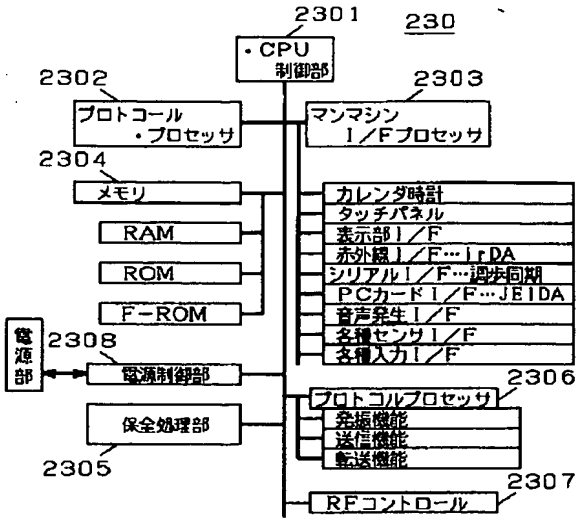
【符号の説明】

１　携帯型電子装置
２ａ，２ｂ，２ｃ　電波通信手段
３　電話機（ＰＨＳ）
３Ａ　電話機
４　中継基地局
１１　受信部（受信手段）
１２　識別部（識別手段）
１３　保全部（保全手段）
２１　発振器
２２　伝送部
２３　微弱電力送信部
２４　微弱電力受信部
２５　伝送部
２６　検波部
２７　判別部
２８　保全手段
３０　公衆ならびに専用回線網
３１　一般の電話機
３２　変復調器付きパソコン
３３　基地局
３４　基地局
３５　基地局
３６　網管理局
４１　発振器
４２　伝送部
４３　微弱電力伝送手段
４４　伝送部
４５　検波部
４６　判別部
４７　保全手段
４８　リセット部
４９　微弱電力受信部
５０　伝送部
５１　検波部
５２　判別部
５３　保全手段
５４　リセット部
５５　発振器
５６　伝送部

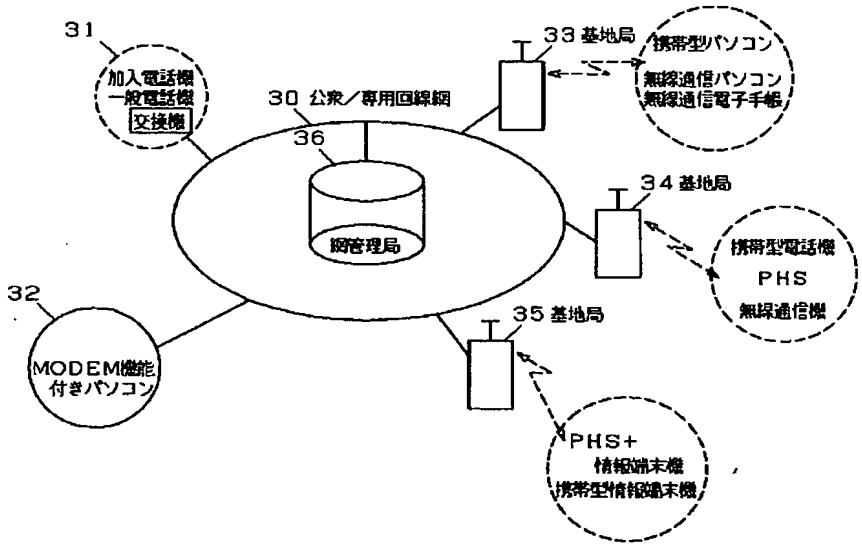
【図１】



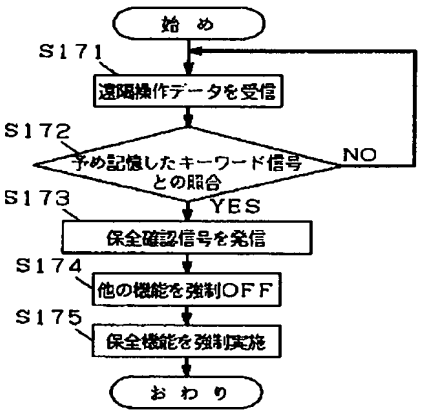
【図３】



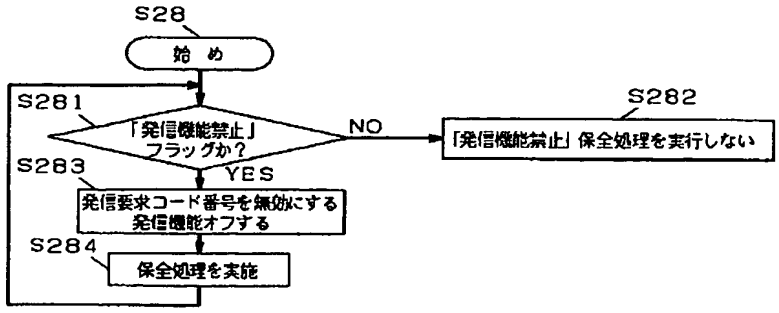
【図４】



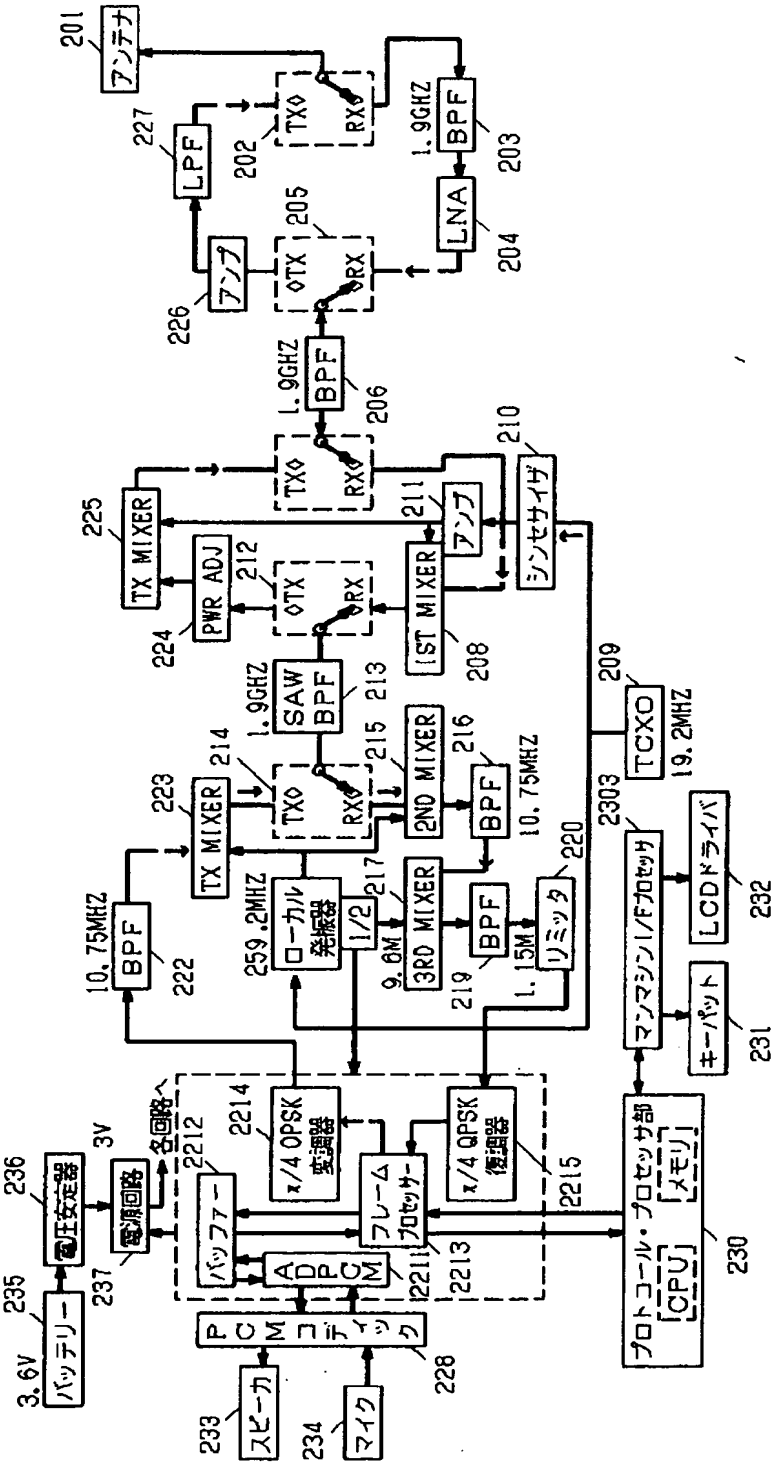
【図１７】



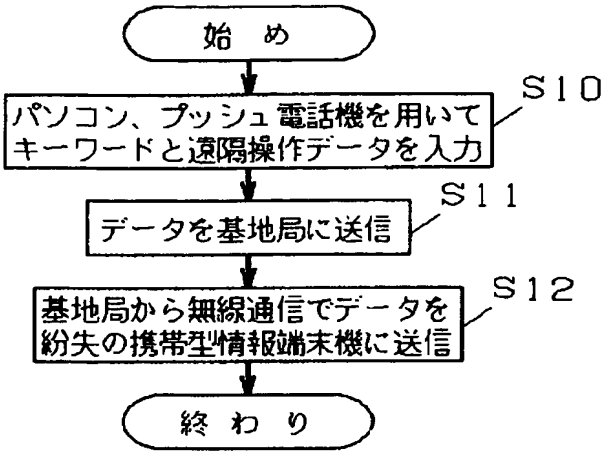
【図１１】



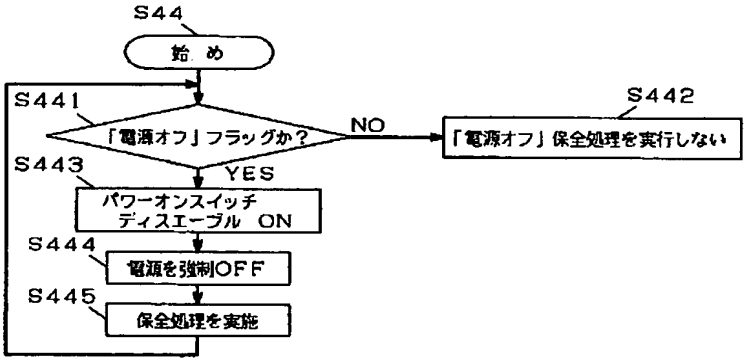
【図２】


201
アンテナ
227
LPF
202
TXΦ
RXΦ
1.9GHZ
BPF
203
LNA
204
205
TX
RX
226
アンプ
L.9GHZ
BPF
206
TXΦ
RXΦ
210
シンセサイザ
225
TX MIXER
PWR ADJ
212
224
TX
RX
211
アンプ
1ST MIXER
208
209
TCXO
19.2MHZ
SAW
BPF
213
1.9GHZ
214
215
2ND MIXER
216
BPF
10.75MHZ
223
TX MIXER
TXΦ
RXΦ
2303
マンマシンI/Fプロセッサ
LCDドライバ
232
キーパット
231
10.75MHZ
BPF
222
259.2MHZ
ローカル発振器
1/2
217
9.6M
3RD MIXER
BPF
219
1.15M
リミッタ
220
2214
π/4 QPSK
変調器
2212
バッファー
フレームプロセッサー
2211
ADPCM
2213
π/4 QPSK
復調器
2215
プロトコール・プロセッサ部
「CPU」「メモリ」
230
236
電圧安定器
3V
電源回路
各回路へ
235
バッテリー
3.6V
237
PCMコーデック
228
233
スピーカ
234
マイク

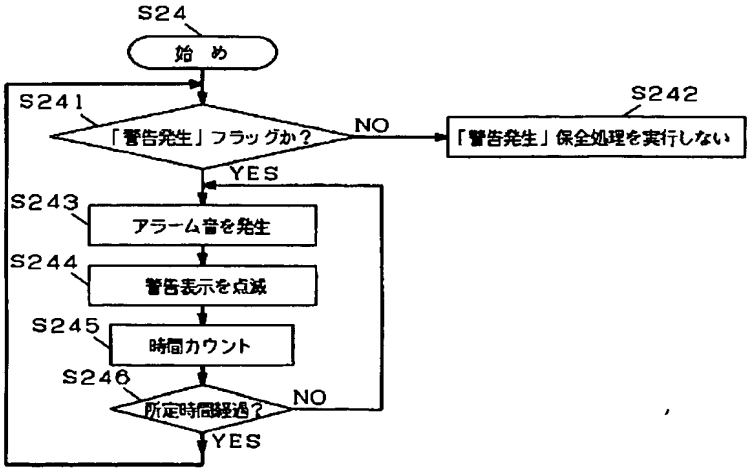
【図５】


始　め
パソコン、プッシュ電話機を用いて
キーワードと遠隔操作データを入力
S10
データを基地局に送信
S11
基地局から無線通信でデータを
紛失の携帯型情報端末機に送信
S12
終　わ　り

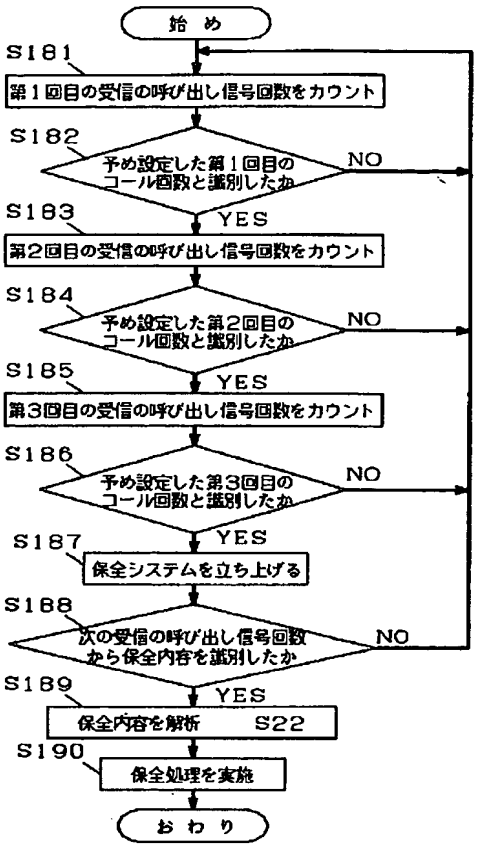
【図７】


S44
始　め
S441
「電源オフ」フラッグか？
NO
S442
「電源オフ」保全処理を実行しない
YES
S443
パワーオンスイッチ
ディスエーブル　ON
S444
電源を強制OFF
S445
保全処理を実施

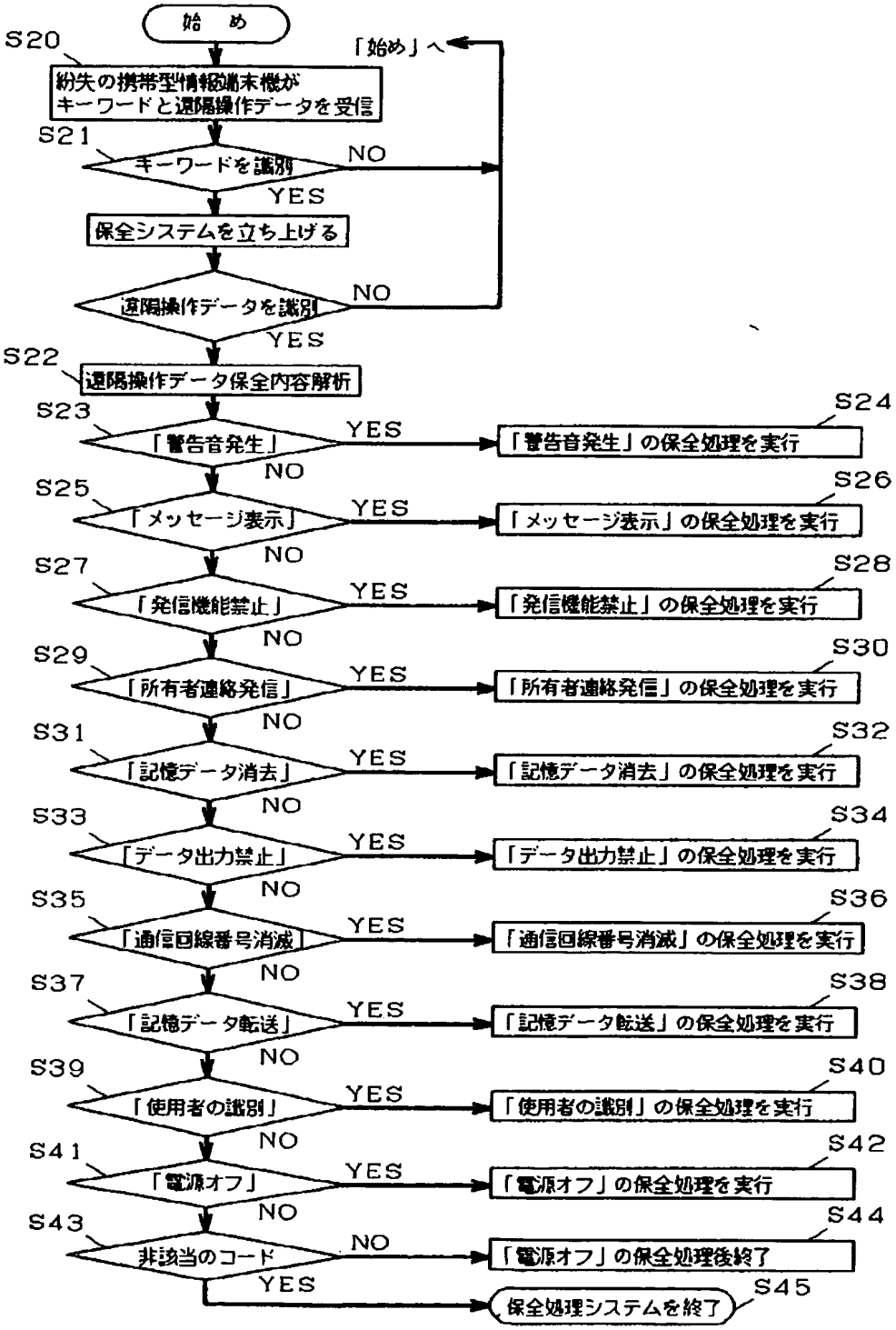
【図８】


S24
始　め
S241
「警告発生」フラッグか？
NO
S242
「警告発生」保全処理を実行しない
YES
S243
アラーム音を発生
S244
警告表示を点滅
S245
時間カウント
S246
所定時間経過？
NO
YES

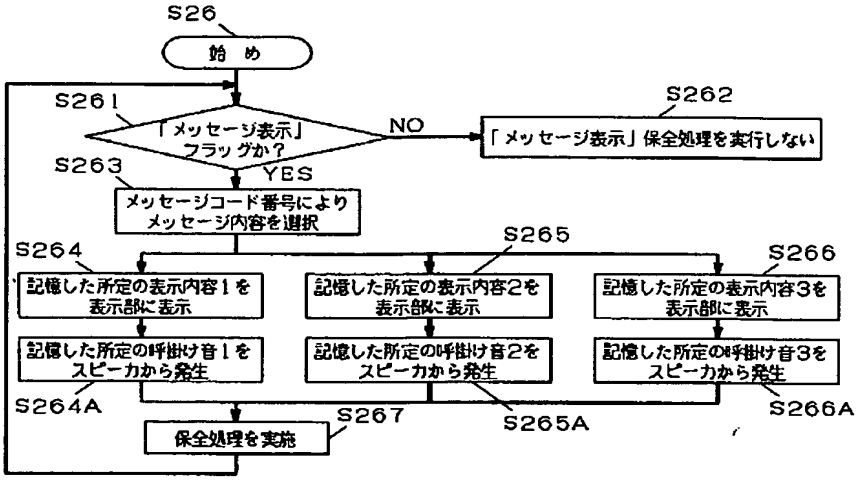
【図１８】


始　め
S181
第１回目の受信の呼び出し信号回数をカウント
S182
予め設定した第１回目の
コール回数と識別したか
NO
YES
S183
第２回目の受信の呼び出し信号回数をカウント
S184
予め設定した第２回目の
コール回数と識別したか
NO
YES
S185
第３回目の受信の呼び出し信号回数をカウント
S186
予め設定した第３回目の
コール回数と識別したか
NO
YES
S187
保全システムを立ち上げる
S188
次の受信の呼び出し信号回数
から保全内容を識別したか
NO
YES
S189
保全内容を解析　　S22
S190
保全処理を実施
おわり

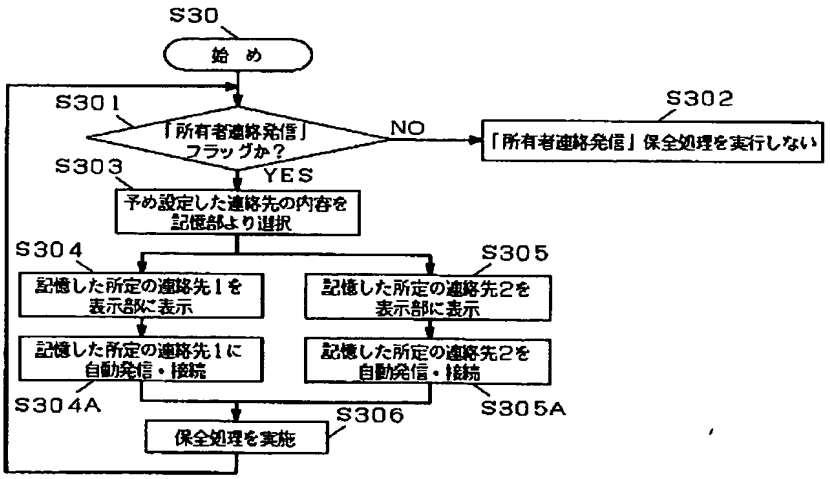
【図６】


始　め
S20
紛失の携帯型情報端末機がキーワードと遠隔操作データを受信
「始め」へ
S21
キーワードを識別
NO
YES
保全システムを立ち上げる
遠隔操作データを識別
NO
YES
S22
遠隔操作データ保全内容解析
S23
「警告音発生」
YES
S24
「警告音発生」の保全処理を実行
NO
S25
「メッセージ表示」
YES
S26
「メッセージ表示」の保全処理を実行
NO
S27
「発信機能禁止」
YES
S28
「発信機能禁止」の保全処理を実行
NO
S29
「所有者連絡発信」
YES
S30
「所有者連絡発信」の保全処理を実行
NO
S31
「記憶データ消去」
YES
S32
「記憶データ消去」の保全処理を実行
NO
S33
「データ出力禁止」
YES
S34
「データ出力禁止」の保全処理を実行
NO
S35
「通信回線番号消滅」
YES
S36
「通信回線番号消滅」の保全処理を実行
NO
S37
「記憶データ転送」
YES
S38
「記憶データ転送」の保全処理を実行
NO
S39
「使用者の識別」
YES
S40
「使用者の識別」の保全処理を実行
NO
S41
「電源オフ」
YES
S42
「電源オフ」の保全処理を実行
NO
S43
非該当のコード
NO
S44
「電源オフ」の保全処理後終了
YES
保全処理システムを終了
S45

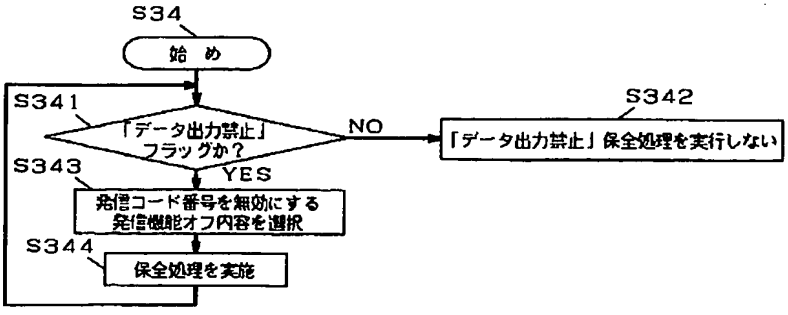
【図９】


S26
始め
S261
「メッセージ表示」フラッグか？
NO
S262
「メッセージ表示」保全処理を実行しない
YES
S263
メッセージコード番号によりメッセージ内容を選択
S264
S265
S266
記憶した所定の表示内容1を表示部に表示
記憶した所定の表示内容2を表示部に表示
記憶した所定の表示内容3を表示部に表示
記憶した所定の呼出け音1をスピーカから発生
記憶した所定の呼出け音2をスピーカから発生
記憶した所定の呼出け音3をスピーカから発生
S264A
S265A
S266A
S267
保全処理を実施

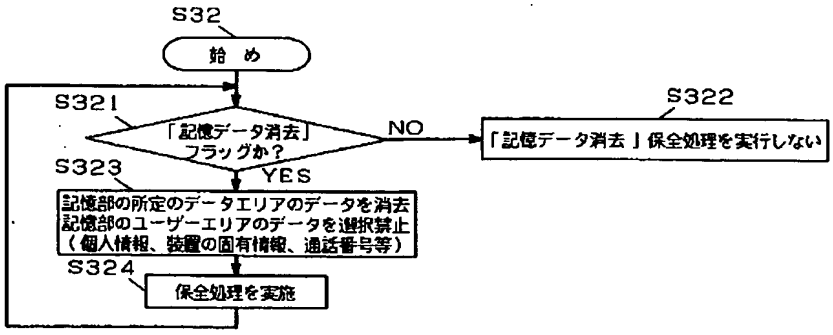
【図１０】


S30
始め
S301
「所有者連絡発信」フラッグか？
NO
S302
「所有者連絡発信」保全処理を実行しない
YES
S303
予め設定した連絡先の内容を記憶部より選択
S304
S305
記憶した所定の連絡先1を表示部に表示
記憶した所定の連絡先2を表示部に表示
記憶した所定の連絡先1に自動発信・接続
記憶した所定の連絡先2を自動発信・接続
S304A
S305A
S306
保全処理を実施

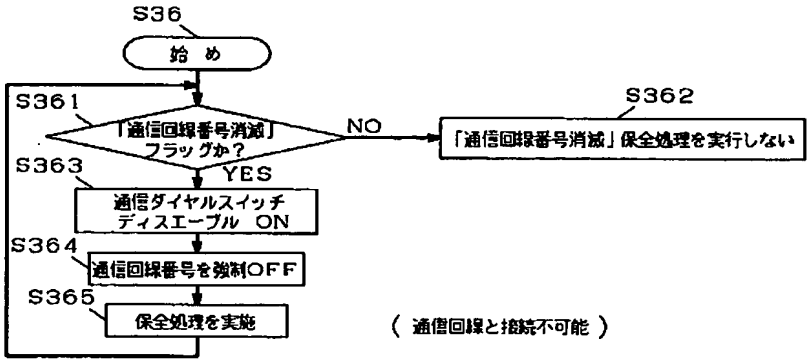
【図１２】


S34
始め
S341
「データ出力禁止」フラッグか？
NO
S342
「データ出力禁止」保全処理を実行しない
YES
S343
発信コード番号を無効にする発信機能オフ内容を選択
S344
保全処理を実施

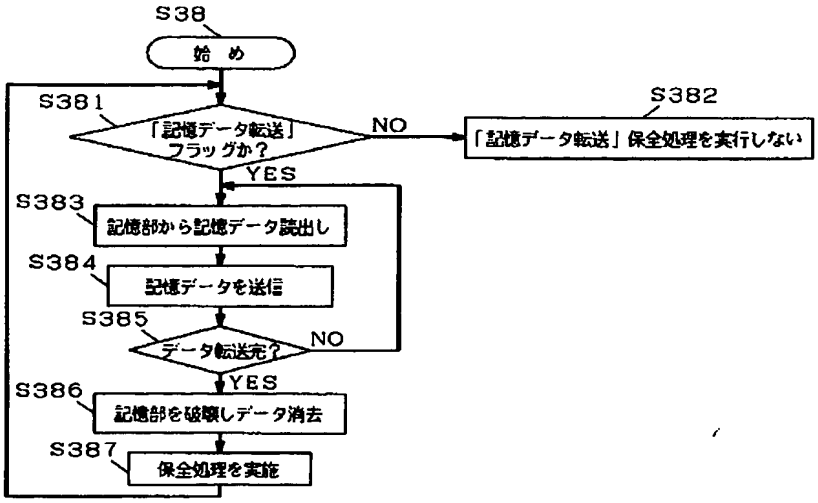
【図１３】


S32
始 め
S321
「記憶データ消去」フラッグか？
NO
S322
「記憶データ消去」保全処理を実行しない
YES
S323
記憶部の所定のデータエリアのデータを消去
記憶部のユーザーエリアのデータを選択禁止
（個人情報、装置の固有情報、通話番号等）
S324
保全処理を実施

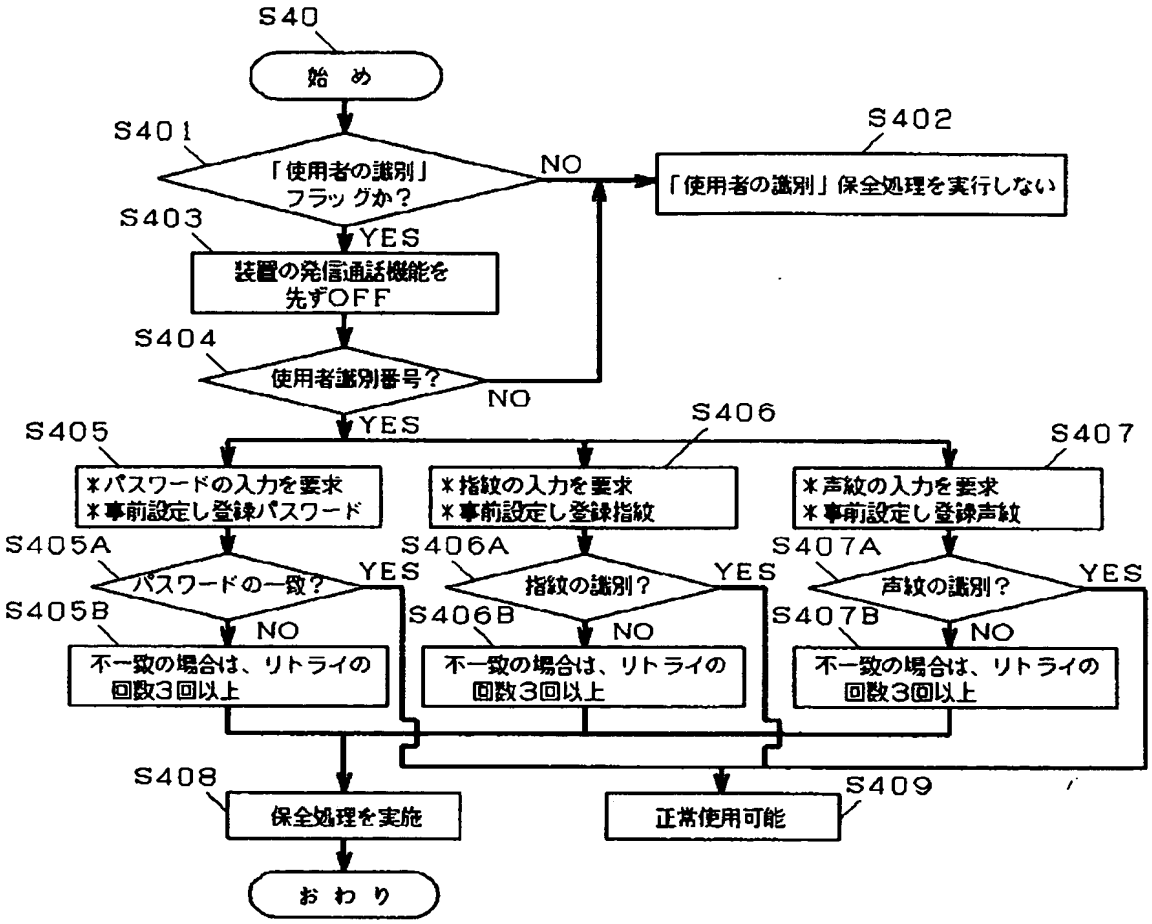
【図１４】


S36
始 め
S361
「通信回線番号消滅」フラッグか？
NO
S362
「通信回線番号消滅」保全処理を実行しない
YES
S363
通信ダイヤルスイッチ
ディスエーブル ON
S364
通信回線番号を強制OFF
S365
保全処理を実施
（通信回線と接続不可能）

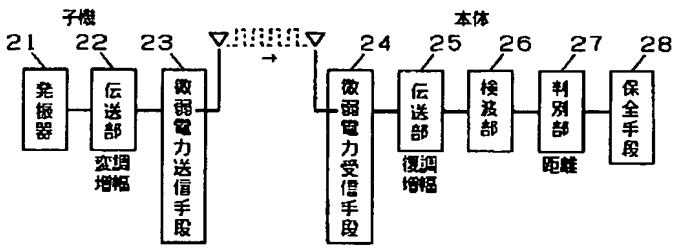
【図１５】


S38
始 め
S381
「記憶データ転送」フラッグか？
NO
S382
「記憶データ転送」保全処理を実行しない
YES
S383
記憶部から記憶データ読出し
S384
記憶データを送信
S385
データ転送完？
NO
YES
S386
記憶部を破壊しデータ消去
S387
保全処理を実施

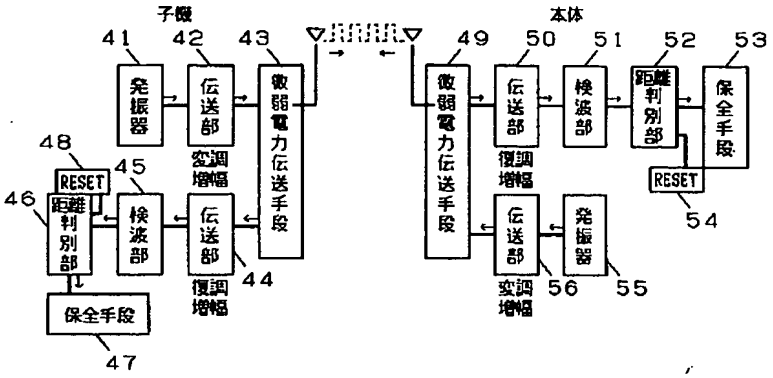
【図１６】


S40
始め
S401
「使用者の識別」フラッグか？
NO
S402
「使用者の識別」保全処理を実行しない
YES
S403
装置の発信通話機能を先ずOFF
S404
使用者識別番号？
NO
YES
S405
＊パスワードの入力を要求
＊事前設定し登録パスワード
S406
＊指紋の入力を要求
＊事前設定し登録指紋
S407
＊声紋の入力を要求
＊事前設定し登録声紋
S405A
パスワードの一致？
YES
NO
S405B
不一致の場合は、リトライの回数3回以上
S406A
指紋の識別？
YES
NO
S406B
不一致の場合は、リトライの回数3回以上
S407A
声紋の識別？
YES
NO
S407B
不一致の場合は、リトライの回数3回以上
S408
保全処理を実施
S409
正常使用可能
お わ り

【図１９】


子機
本体
21
22
23
24
25
26
27
28
発振器
伝送部
変調増幅
微弱電力送信手段
微弱電力受信手段
伝送部
復調増幅
検波部
判別部
距離
保全手段

【図２０】


子機
本体
41
42
43
49
50
51
52
53
発振器
伝送部
変調増幅
微弱電力伝送手段
微弱電力伝送手段
伝送部
復調増幅
検波部
距離判別部
保全手段
48
RESET
45
46
距離判別部
検波部
伝送部
復調増幅
44
伝送部
変調増幅
発振器
56
55
RESET
54
保全手段
47